A Guide to Forensic Accounting Investigation

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Australia and Asia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Finance series contains books written specifically for finance and investment professionals as well as sophisticated individual investors and their financial advisors. Book topics range from portfolio management to e-commerce, risk management, financial engineering, valuation and financial instrument analysis, as well as much more.

For a list of available titles, visit our Web site at www.WileyFinance.com.

A Guide to Forensic Accounting Investigation

Second Edition

THOMAS W. GOLDEN
STEVEN L. SKALAK
MONA M. CLAYTON
JESSICA S. PILL

WILEY
John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

A guide to forensic accounting investigation – 2nd ed. / Thomas W. Golden ... [et al.].
p. cm.
Rev. ed. of: Guide to forensic accounting investigation / Thomas W. Golden, Steven L. Skalak, Mona M. Clayton. 2006.
Includes index.
ISBN 978-0-470-59907-5 (hardback)
1. Fraud investigation–Auditing. 2. Forensic investigation–Auditing. I. Golden, Thomas W. II. Golden, Thomas W. Guide to forensic accounting investigation.
HV8079.F7G84 2011
363.25′963–dc22 2010043319

ISBN-13: 978-0-470-59907-5

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The catastrophic business failures of this decade have been revealing on many levels. From my professional perspective as a forensic accounting investigator, I couldn't help but notice the need across much of the business community for a better grasp of the scope and skills of the forensic accounting investigator. Most people seemed to be struggling. How could these massive frauds have occurred? How can such events be deterred—if not wholly prevented—in the future? Who is responsible for deterrence, detection, and investigation? Is it a matter of systems, of attitudes, of aggressive internal policing, of more stringent regulatory oversight, of "all of the above," and more still? What methods are effective? What should an auditor, a corporate director, an executive look for? There were far more questions than answers, and all the questions were difficult. Forensic accounting investigation had become important to the larger business community and the public. They were relying on it to solve problems, deter new problems, and contribute to new, tougher standards of corporate behavior and reported information. But all concerned, from CEOs to financial statement auditors, still have much to learn about the relatively new discipline of forensic accounting investigation.

The keynotes of the past ten years are tough new legislation and regulation to strengthen corporate governance and new oversight of the financial community, corporations, and auditors. Also, the accounting profession continues to review the need for new and different approaches to fraud. All of these initiatives are intended to increase investor confidence in corporate information and financial markets.

Pushing these trends relentlessly forward is the conviction of the concerned public that corporate fraud is unacceptable. It may well occur—this is an imperfect world—but everything must be done to deter, detect, investigate, and penalize it. Investors look to corporate directors and executives, internal and external auditors, and regulators to keep companies honest. They want to be able to trust securities analysts to report and recommend without concealed self-interest. And they expect lenders, business partners, and others who deal with a corporation to exercise and require sound business ethics.

Where fraud is concerned, there is no silver bullet. Clearly, a book would help to address the needs of three broad constituencies: management, corporate directors, and auditors (internal and external). Just as clearly, it shouldn't be a book that focused only on concepts and facts. It would need to look at practice. It would have to convey effective working attitudes and realistic perspectives on many issues, from the varied skills required of forensic accounting investigators to working with attorneys and reporting findings. It would have to offer case studies that reveal the thinking of both experienced investigators and the fraudsters they pursue. In short, it would have to bring its readers into the complex and evolving culture of

forensic accounting investigation while serving as a comprehensive, reliable, easily used reference source.

This is a book that some readers will explore page by page; others will use it as a reference. However it is approached, it will reveal the complexity of fraud deterrence, detection, and investigation and offer a step-by-step method to understanding that complexity. Some readers will seek in this book a broad appreciation for investigative techniques so that they can more effectively manage the process when and if needed. Others will want to commit the details to memory. For both types of reader, it is all here: common fraudulent schemes, the psychology of the fraudster, the need for professional skepticism, responding to whistle-blowers, working with lawyers and prosecutors, new technologies that facilitate detection, and much more.

In practical reality, no one can guarantee that all frauds will be either prevented or detected in a timely manner. Yet the toolbox of those who safeguard the integrity of corporate information and investigate possible wrongdoing is well filled. This book will make that clear. It puts before the reader what is, to my mind, an extraordinary array of best practices, tools, and techniques for the deterrence, detection, and investigation of corporate fraud. The skills and knowledge of the forensic accounting investigator are evident on every page.

This is by no means a casual book, tossed off to meet an ephemeral need. We hope that the effort that has gone into it will make it substantively useful over the long term. With proper knowledge and diligence among all those who are responsible for providing financial information for the capital markets, financial fraud can be significantly deterred. As the suspicion and reality of fraud diminish across the corporate world, investors will regain confidence in the integrity of corporate information. The ultimate purpose of this book reaches past the audit profession—and the directors and managers who hire and work with auditors—to address the needs of the capital markets worldwide.

Steven L. Skalak, Partner
Mona M. Clayton, Partner
Thomas W. Golden, Partner, Retired
Jessica S. Pill, Director, Forensic Services
PricewaterhouseCoopers LLP

Acknowledgments

A book of this scope is a collective endeavor. We want to take this opportunity to thank Dennis Nally, Juan Pujadas, Greg Bardnell, and Greg Garrison. We want also to identify those individuals who have contributed to a sustained effort of thinking, writing, fact-checking, editing, and project management.

There was a team around us from the beginning. We owe a particular debt of gratitude to Robbie Pound. This is a better book for his counsel and suggestions. Meredith Kochanek and Molly McCarthy, serving as co-project managers, were indispensable and kept us focused on the next mountain to climb, ensuring thorough communication as we progressed. At John Wiley & Sons, we benefited from the patience and acumen—as they well know—of Robert Chiarelli, John DeRemigis, Jennifer MacDonald, Kelly O'Connor, and their colleagues.

We owe particular gratitude to our Chicago- and New York–based practice teams. The directors, managers, staff, and assistants with whom we work closely, as well as many other colleagues, performed research, checked exhibits, read chapters, chased facts, and provided insights. Their tireless effort and enthusiasm energized us each day in the conviction that this book will be useful to many people in these challenging times.

Our greatest thanks go to our fellow authors—practitioners in the United States and around the world, and a number of attorneys with other firms or government, who drew on their time, experience, and wisdom to write many of the chapters. At the head of each chapter, readers will find these individuals clearly and gratefully identified. This is their book as much as it is ours.

The following roster names, with gratitude, the authors who created the original drafts of all chapters and approved their final form. All are partners or employees of PricewaterhouseCoopers apart from clearly identified exceptions.

1. Fraud: An Introduction
   Steven L. Skalak
   Manny A. Alas
   Gus Sellitto
2. Psychology of the Fraudster
   Thomas W. Golden
3. The Roles of the Auditor and the Forensic Accounting Investigator
   James S. Gerson
   John P. Brolly
   Steven L. Skalak
4. Auditor Responsibilities and the Law
   Geoffrey Aronow, Partner, Bingham McCutchen LLP, Washington, D.C.
   Hartwell Harris, Associate, Bingham McCutchen LLP, Santa Monica, CA

5. When and Why to Call in Forensic Accounting Investigators
   Darren J. Tapp
   W. McKay (Mac) Henderson
6. Internal Audit: The Second Line of Defense
   Dennis D. Bartolucci
   Therese M. Bobek
   James A. LaTorre
7. Teaming with Forensic Accounting Investigators
   Erik Skramstad
8. Anonymous Communications
   W. McKay (Mac) Henderson
   Peter J. Greaves
9. Personal Privacy and Public Disclosure
   Hugo Teufel III
   Sanjay Subramanian
   Sergio Pedro
10. Building a Case: Gathering and Documenting Evidence
    Frederic R. Miller
    David L. Marston
11. Independence, Objectivity, Skepticism
    Steven L. Skalak
    Thomas W. Golden
12. Potential Missteps: Considerations When Fraud Is Suspected
    Thomas W. Golden
    Kevin D. Kreb
13. Potential Red Flags and Fraud Detection Techniques
    Will Kenyon
    Patricia D. Tilton
14. Investigative Techniques
    Mona M. Clayton
15. Corporate Intelligence
    David Jansen
    Glenn Ware
    Alexander Kapur
16. The Art of the Interview
    Thomas W. Golden
    Michael T. Dyer
17. Data Mining
    Dyan Decker
    Alexandre Blanc
    John Loveland
    Mona Clayton
18. Report of Investigation
    Thomas W. Golden
    Ryan D. Murphy
19. Supporting a Criminal Prosecution
    Albert A. Vondra
    Thomas W. Golden

John Gallo, Partner, Sidley Austin Brown and Wood LLP, Chicago
Isabel M. Cumming, Chief of Economic Crimes, Prince George's County, Maryland

20. Working with Attorneys
Thomas W. Golden
Michael T. Dyer
Sonya Andreassen-Henderson

21. Financial Reporting Fraud and Capital Markets
Daniel V. Dooley
Steven L. Skalak

22. Financial Statement Fraud: Revenue and Receivables
Jonny J. Frank
David Jansen
Michael Carey

23. Financial Statement Fraud: Other Schemes and Misappropriations
Jonny J. Frank
David Jansen
Michael Carey

24. Ponzi Schemes
Steven L. Skalak
Regina Lau
Sherrie Clarke

25. Money Laundering
Andrew P. Clark
Marie-Alice Hofmaier
Christopher Cowin

26. Foreign Corrupt Practices Act
Sulaksh Shah
Dana Weintraub
Frederic R. Miller

27. Construction Projects
Daryl Walcroft
Anthony Morgan

28. Contract Compliance
Jeff Leedom
Philip Treccagnoli
David L. Marston

29. Other Dimensions of Forensic Accounting
Michael S. Markman
Aron Levko
Mark W. Haller
Robert W. Dennis
Mona M. Clayton
J. Christopher Dineen
Dyan Decker
Shane Sims

30. Corporate Remediation
Matthew J. Shelhorse
Christopher D. Barbee
Peter A. Viksnins
Faizal B. Karim

The authors offer this book with the hope that it answers a very real need and will provide its readers with a new and compelling vision of the role of forensic accountants in the deterrence, detection, and investigation of corporate fraud. The views expressed in this book are those of the individual authors and are not necessarily the views of PricewaterhouseCoopers or any other PricewaterhouseCoopers partner or employee. Unless otherwise indicated, the authors are not attorneys and their comments are based on their personal experiences and do not represent legal advice.

THOMAS W. GOLDEN
STEVEN L. SKALAK
MONA M. CLAYTON
JESSICA S. PILL

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 1

Fraud: An Introduction

Steven L. Skalak, Manny A. Alas, and Gus Sellitto

Fraud evokes a visceral reaction in us. It is an abuse of our expectation of fair treatment by fellow human beings. Beyond that, it is a blow to our self-image as savvy managers capable of deterring or detecting a fraudulent scheme. Whether we react because of our values or our vanity, nobody likes to be duped. Many elements of modern society are focused on maintaining an environment of fair dealing. Laws are passed; agencies are established to enforce them; police are hired; ethics and morals are taught in schools and learned in businesses; and criminals are punished by the forfeiture of their ill-gotten gains and personal liberty—all with a view to deterring, detecting, and punishing fraud. The profession of accounting and auditing grew out of society's need to ensure fair and correct dealings in commerce and government.

One of the central outcomes of fraud is financial loss. Therefore, in the minds of the investing public, the accounting and auditing profession is inextricably linked with fraud deterrence, fraud detection, and fraud investigation. This is true to such an extent that there are those whose perception of what can be realistically accomplished in an audit frequently exceeds the services that any accountant or auditor can deliver and, in terms of cost, exceeds what any business might be willing to pay (see Chapter 3). In the past decade, public anger over occurrences of massive fraud in public corporations and the conduct of financial institutions has spawned substantial government spending, regulatory reform, global convergence of accounting standards, new auditing standards, new oversight of the accounting profession, and greater penalties for those who conspire to commit or conceal financial fraud or act corruptly.

This book addresses the distinct roles of corporate directors, management, external auditors, internal auditors, and forensic accounting investigators with respect to fraud deterrence, fraud detection, and fraud investigation.[1] As will quickly become

[1] *Forensic accountants* are members of a broad group of professionals that includes but is not limited to those who perform financial investigations. The public often uses the term *forensic accountants* to refer to financial investigators, although many forensic accountants do not perform financial investigations. In Chapter 29, we discuss the many other services encompassed under the broader term *forensic accounting*. A forensic accounting investigator is trained and experienced in investigating and resolving suspicions or allegations of fraud through document analysis to include both financial and nonfinancial information, interviewing, and third-party

apparent later in this introductory chapter, these professionals are by no means the only ones concerned with combating fraud. However, each has a significant role in the larger effort to minimize fraud.

FRAUD: WHAT IS IT?

Generally, all acts of fraud can be distilled into four basic elements:

1. A false representation of a material nature[2]
2. Scienter—knowledge that the representation is false, or reckless disregard for the truth
3. Reliance—the person receiving the representation reasonably and justifiably relied on it
4. Damages—financial damages resulting from all of the foregoing

By way of illustration, consider the classic example of the purchase of a used car. The salesperson is likely to make representations about the quality of the car, its past history, and the quality of parts subject to wear and tear, ranging from the transmission to the paint job. The elements of fraud may or may not arise out of such statements. First, there is a distinction between hype and falsehood. The salesperson hypes when he claims that the 1977 Chevy Vega "runs like new." However, were he to turn back the odometer, he would be making a false representation. Second, the false statement must be material. If the odometer reading is accurate, the salesperson's representation that the car runs like new or was only driven infrequently, is, strictly speaking, mere hype: The purchaser need only look at the odometer to form a prudent view of the extent of use and the car's likely roadworthiness. Third, the fraudster must make the material false misrepresentation with *scienter,* that is, with actual knowledge that the statement is false or with a reckless disregard for the truth. For example, the car may or may not have new tires. But if the salesperson, after making reasonable inquiries, truly believes that the Vega has new tires, there is no knowing misrepresentation. There may be negligence, but there is no fraud. Fourth, the potential victim must justifiably rely on the false representation. A buyer who wants a blue car may actually believe the salesperson's representation that "it's really blue but looks red in this light." Reliance in that case is, at best, naive and certainly not justified. Finally, there must be some form of damage. The car must in fact prove to be a lemon when the purchaser drives off in it and realizes that he has been misled. Regardless of context, from Enron, Siemens, or Countrywide to

inquiries, including commercial databases. See the Auditing and Investigation section at the end of this chapter. *Auditors* is used throughout this text to represent both internal and external auditors unless otherwise specified as pertaining to one group or the other.

[2] The term *material* as used in this context is a legal standard whose definition varies from jurisdiction to jurisdiction. It should not be confused with the concept of materiality as used in auditing, in which one considers the effect of fraud and errors related to financial statement reporting.

Honest Abe's Used Car Lot, fraud is fraud, and it displays the four simple elements noted earlier.

FRAUD: PREVALENCE, IMPACT, AND FORM

Fraud is a feature of every organized culture in the world. It affects many organizations, regardless of size, location, or industry. According to the Association of Certified Fraud Examiners' survey, approximately $994 billion was lost by U.S. companies in 2008 due to occupational fraud and abuse, and over one in four cases cost the organization in excess of $1 million.[3] Twenty-nine percent of all fraud is committed by accounting department employees, and 18 percent of frauds were committed by members of upper management.[4] According to PwC's 2009 Securities Litigation Study, senior officers of companies continue to be named in the majority of filings during 2009. The percentage of U.S. federal securities class action lawsuits naming the CEO, CFO, chairman, and president were 81 percent, 62 percent, 47 percent, and 62 percent, respectively.[5]

If one were to look at the FBI's statistics for white-collar crime, however, one would not reach this conclusion because those statistics are based upon prosecutions and, as discussed in Chapter 19, "Supporting a Criminal Prosecution," the overwhelming majority of frauds are not prosecuted. Based upon our own experience as well as on surveys conducted by PricewaterhouseCooper (hereafter referred to throughout as PwC) (PwC Economic Crime Survey) and the Association of Certified Fraud Examiners (ACFE), we believe that fraud is pervasive.

According to the 2009 PwC Global Economic Crime Survey statistics, 30 percent of organizations fell victim to fraud over the previous 12 months. This is compared to 43 percent in 2007 and 45 percent in 2005, which both look back two years.[6] Respondents from Eastern and Western Europe were among the companies reporting the highest incidents of fraud; for example, 71 percent of organizations in Russia and 43 percent in the United Kingdom reported having experienced fraud in their organization.[7] Across all companies surveyed, 27 percent said that the direct financial impact of fraud exposure was more than $500,000, and 25 percent of those reporting

---

[3] U.S. organizations lose an estimated 7 percent of their annual revenues to fraud, according to a survey of Certified Fraud Examiners who investigated cases between January 2006 and February 2008. When applied to the projected 2008 U.S. Gross National Product, the 7 percent figure translates to approximately $994 billion in fraud losses. The full study can be found at: www.acfe.com/RTTN/2008-rttn.asp. Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2004), ii.

[4] Id.

[5] PricewaterhouseCoopers *Securities Litigation Study 2009*.

[6] PricewaterhouseCoopers, *Global Economic Crime Survey 2007,* 4, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/pwc_2007gecs.pdf.

[7] PricewaterhouseCoopers, *Global Economic Crime Survey 2009,* 10, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf.

accounting fraud believed that it had cost them more than $1 million.[8] Overall, the reality of fraud is greater than the perception. Statistics from our 2007 survey show that 13 percent and 6 percent of respondents thought it was likely that they would experience asset misappropriation and accounting fraud, respectively, over the next two years. Interestingly, those numbers may be low, given that in our 2009 survey, 20 percent of companies reported being victims of asset misappropriation and 11 percent reported having experienced accounting fraud.[9]

FRAUD IN HISTORICAL PERSPECTIVE

Fraud in one form or another has been a fact of business life for thousands of years. In Hammurabi's Babylonian Code of Laws, dating to approximately 1800 B.C.E., the problem of fraud is squarely faced: "If a herdsman, to whose care cattle or sheep have been entrusted, be guilty of fraud and make false returns of the natural increase, or sell them for money, then shall he be convicted and pay the owner ten times the loss."[10] The earliest lawmakers were also the earliest to recognize and combat fraud.

In the United States, frauds have been committed since the colonies were settled. A particularly well-known fraud of that era was perpetrated in 1616 in Jamestown, Virginia, by Captain Samuel Argall, the deputy governor. Captain Argall allegedly "fleeced investors in the Virginia Co. of every chicken and dry good that wasn't nailed down."[11] According to the book *Stealing from America,* within two years of Argall's assumption of leadership in Jamestown, the "whole estate of the public was gone and consumed. . . ."[12] When he returned to England with a boat stuffed with looted goods, residents and investors were left with only six goats.[13]

Later, during the American Civil War, certain frauds became so common that legislatures recognized the need for new laws. One of the most egregious frauds was to bill the United States government for defective or nonexistent supplies sold to the Union Army. The federal government's response was the False Claims Act, passed in March 1863, which assessed corrupt war profiteers double damages and a $2,000 civil fine for each false claim submitted. Remarkably enough, this law is still in force, though much amended.

Soon after the Civil War, another major fraud gained notoriety: the Crédit Mobilier scheme of 1872. Considered the most serious political scandal of its time, this fraud was perpetrated by executives of the Union Pacific Railroad Company, operating in conjunction with corrupt politicians. Crédit Mobilier of America was set up by railroad management and by Representative Oakes Ames of Massachusetts,

[8] Id., 13.
[9] Id., 18.
[10] *Hammurabi's Code of Laws* (1780 B.C.E.), L. W. King, trans.
[11] Carol Emert, "A Rich History of Corporate Crime; Fraud Dates Back to America's Colonial Days," the *San Francisco Chronicle,* July 14, 2002.
[12] Id.
[13] Id.

ostensibly to oversee construction of the Union Pacific Railroad.[14] Crédit Mobilier charged Union Pacific (which was heavily subsidized by the government) nearly twice the actual cost of completed work and distributed the extra $50 million to company shareholders.[15] Shares in Crédit Mobilier were sold at half price, and at times offered gratis, to congressmen and prominent politicians for the purpose of buying their support. Among the company's famous shareholders were Vice President Schuyler Colfax, Speaker of the House James Gillespie Blaine, future vice presidents Henry Wilson and Levi Parsons Morton, and future president James Garfield.[16]

TYPES OF FRAUD

There are many different types of fraud, and many ways to characterize and catalog fraud; those of the greatest relevance to accountants and auditors, however, are the following broad categories:

- *Employee Fraud*[17]*/Misappropriation of Assets.* This type of fraud involves the theft of cash or inventory, skimming revenues, payroll fraud, and embezzlement. Asset misappropriation is the most common type of fraud.[18] Primary examples of asset misappropriation are fraudulent disbursements such as billing schemes, payroll schemes, expense reimbursement schemes, check tampering, and cash register disbursement schemes. Sometimes employees collude with others to perpetrate frauds, such as aiding vendors intent on overbilling the company. An interesting distinction: Some employee misdeeds do not meet the definition of fraud because they are not schemes based on communicating a deceit to the employer. For example, theft of inventory is not necessarily a fraud—it may simply be a theft. False expense reporting, on the other hand, is a fraud because it involves a false representation of the expenses incurred. This fraud category also includes employees' aiding and abetting others outside the company to defraud third parties.
- *Financial Statement Fraud.* This type of fraud is characterized by intentional misstatements or omissions of amounts or disclosures in financial reporting to deceive financial statement users. More specifically, financial statement fraud involves manipulation, falsification, or alteration of accounting records or supporting documents from which financial statements are prepared. It also refers to the intentional misapplication of accounting principles to manipulate results.

---

[14] Id.

[15] Peter Carlson, "High and Mighty Crooked: Enron Is Merely the Latest Chapter in the History of American Scams," *The Washington Post,* February 10, 2002.

[16] D. C. Shouter, "The Crédit Mobilier of America: A Scandal that Shook Washington," *Chronicles of American Wealth,* No. 4, November 30, 2001, www.raken.com/american_wealth/other/newsletter/chronicle301101.asp.

[17] *Employee* here refers to all officers and employees who work for the organization.

[18] Association of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2008), 11.

> According to a study conducted by the Association of Certified Fraud Examiners, fraudulent financial statements, as compared with the other forms of fraud perpetrated by corporate employees, usually have a higher dollar impact on the victimized entity as well as a more negative impact on shareholders and the investing public.[19]

As a broad classification, corruption straddles both misappropriation of assets and financial statement fraud. Transparency International, a widely respected not-for-profit think tank, defines corruption as "the abuse of entrusted power for private gain."[20] We would expand that definition to include corporate gain as well as private gain. Corruption takes many forms and ranges from executive compensation issues to payments made to domestic or foreign government officials and their family members. Corrupt activities are prohibited in the United States by federal and state laws. Beyond U.S. borders, contributions to foreign officials are prohibited by the Foreign Corrupt Practices Act.

This book is primarily concerned with fraud committed by employees and officers, some of which may lead to the material distortion of financial statement information, and the nature of activities designed to deter and investigate such frauds. Circumstances in which financial information is exchanged (generally in the form of financial statements) as the primary representation of a business transaction are fairly widespread. They include, for example, regular commercial relationships between a business and its customers or vendors, borrowing money from banks or other financial institutions, buying or selling companies or businesses, raising money in the public or private capital markets, and supporting the secondary market for trading in public company debt or equity securities. This book focuses primarily on three types of fraud:

1. Frauds perpetrated by people within the organization that result in harm to the organization itself
2. Frauds committed by those responsible for financial reporting, who use financial information they know to be false so they can perpetrate a fraud on investors or other third parties, whereby the organization benefits
3. Corrupt acts by companies or their executives, whereby the executive personally or the company benefits

ROOT CAUSES OF FRAUD

As society has evolved from barter-based economies to e-commerce, so has fraud evolved into complex forms—Hammurabi's concern about trustworthy shepherds was just the beginning. In the early 2000s, companies headquartered in the developed world took the view that their business risk was highest in emerging, or Third World

[19] Id.
[20] Transparency International, "TI's Vision, Mission, Values, Approach and Strategy," www.transparency.org.

regions, where foreign business cultures and less-developed regulatory environments were believed to generate greater risk.[21] Gaining market access and operating in emerging or less-developed markets seemed often enough to invite business practices that were wholly unacceptable at home. Sharing this view, the governments of major industrial countries enacted legislation to combat the potential for corruption. The United States enacted the Foreign Corrupt Practices Act (FCPA); countries working together in the Organisation for Economic Co-operation and Development (OECD) enacted the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (known as the *OECD Convention*); the United Nations adopted the United Nations Convention against Corruption (UNCAC); Canada enacted the Corruption of Foreign Public Officials Act; and the United Kingdom passed its Bribery Act in 2010.

This way of thinking about risk and markets and of combating corruption and fraud is no longer adequate, however. The new paradigm for understanding risk postulates that fraud risk factors are borderless and numerous. Fraud is now understood to be driven by concerns over corporate performance, financing pressures including access to financing, the competition to enter and dominate markets, legal requirements and exposure, and personal needs and agendas.[22] The need for this new paradigm has become increasingly clear in the past few years, when the greatest risk to investors has appeared to be participation in the seemingly well-regulated and well-established U.S. and European markets. More recently, events at several major European multinationals have shown that the risk of massive fraud and corruption knows no borders.

The recent spate of Ponzi schemes, corruption, and financial scandals has demonstrated that large-scale corporate improprieties can and do occur in sophisticated markets; they are by no means the exclusive province of foreign or remote markets. Capital market access and the related desire of listed companies to boost revenue growth, and investors' desire to achieve significant and stable returns, through whatever means necessary, are major factors contributing to financial malfeasance worldwide.

A HISTORICAL ACCOUNT OF THE AUDITOR'S ROLE

We have briefly examined the elements, forms, and evolution of fraud. We can now examine the role of one of the key players in the effort to detect fraud, the auditor.

Auditing: Ancient History

Historians believe that recordkeeping originated about 4000 B.C.E., when ancient civilizations in the Near East began to establish organized governments and

[21] PricewaterhouseCoopers, "Financial Fraud—Understanding Root Causes," *Investigations and Forensic Services Report* (2002), 1.
[22] PricewaterhouseCoopers, *Global Economic Crime Survey 2007*, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/pwc_2007gecs.pdf.

businesses.[23] Governments were concerned about accounting for receipts and disbursements and collecting taxes. An integral part of this concern was establishing controls, including audits, to reduce error and fraud on the part of incompetent or dishonest officials.[24] There are numerous examples in the ancient world of auditing and control procedures employed in the administration of public finance systems. The Shako dynasty of China (1122–256 B.C.E.), the assembly in classical Athens, and the Senate of the Roman Republic all exemplify early reliance on formal financial controls.[25]

Much later, in the twelfth and thirteenth centuries, records show that auditing work was performed in England, Scotland, Italy, and France. The audits in Great Britain performed before the seventeenth century were directed primarily at ensuring the accountability of funds entrusted to public or private officials.[26] Those audits were not designed to test the quality of the accounts, except insofar as inaccuracies might point to the existence of fraud.

Economic changes between 1600 and 1800, which saw the beginning of widespread commerce, introduced new accounting concerns focused on the ownership of property and the calculation of profit and loss in a business sense. At the end of the seventeenth century, the first law prohibiting certain officials from serving as auditors of a town was enacted in Scotland, thus introducing the modern notion of auditor independence.[27]

Growth of the Auditing Profession in the Nineteenth Century

It was not until the nineteenth century, with the growth of railroads, insurance companies, banks, and other joint stock companies, that the auditing profession became an important part of the business environment. In Great Britain, the passage of the Joint Stock Companies Act in 1844 and later the Companies Act in 1879 contributed greatly to the auditing field in general and to the development of external auditing in the United States.[28] The Joint Stock Companies Act required companies to make their books available for the critical analysis of shareholders at the annual meeting. The Companies Act in 1879 required all limited liability banks to submit to auditing, a requirement later expanded to include all such companies.[29] Until the beginning of the twentieth century, independent audits in the United States were modeled on British practice and were in fact conducted primarily by auditors from

[23] Robert Hiester Montgomery, *Montgomery's Auditing,* 12th ed. (New York: John Wiley & Sons, 1998), 1–7.
[24] Id.
[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Dr. Sheri Markose, "Honest Disclosure, Corporate Fraud, Auditors and Stock Market Valuation," lecture from course EC247: "Financial Instruments and Capital Market Institutions," University of Essex (Essex, U.K., 2003).

Britain, who were dispatched overseas by British investors in U.S. companies. British-style audits, dubbed "bookkeeper audits," consisted of detailed scrutiny of clerical data relating to the balance sheet. These audits were imperfect at best. J. R. Edwards, in *Legal Regulation of British Company Accounts, 1836–1900,* cites the view of Sir George Jessel, a lawyer and judge famous in his day, on the quality of external auditing soon after passage of the Companies Act:

> *The notion that any form of account will prevent fraud is quite delusive. Anybody who has had any experience of these things knows that a rogue will put false figures into an account, or cook as the phrase is, whatever form of account you prescribe. If anybody imagines that will protect the shareholders, it is simply a delusion in my opinion. . . . I have had the auditors examined before me, and I have said, "You audited these accounts?" "Yes." "Did you call for any vouchers?" "No, we did not; we were told it was all right, we supposed it was, and we signed it."*[30]

Yet by the end of the nineteenth century, the most sophisticated minds in the auditing field were certain that auditors could do much better than this. Witness the incisive view of Lawrence R. Dicksee, author of a manual widely studied in its day (and still available today, many editions later):

> *The detection of fraud is the most important portion of the Auditor's duties, and there will be no disputing the contention that the Auditor who is able to detect fraud is—other things being equal—a better man than the auditor who cannot. Auditor[s] should, therefore, assiduously cultivate this branch of their functions. . . .*[31]

In response to the rapidly expanding American business scene, audits in the United States evolved from the more cumbersome British practice into "test audits." According to *Montgomery's Auditing,* the emergence of independent auditing was largely due to the demands of creditors, particularly banks, for reliable financial information on which to base credit decisions.[32] That demand evolved into a series of state and federal securities acts, which significantly increased a company's burden to publicly disclose financial information and, accordingly, catapulted the auditor into a more demanding and visible role.

Federal and State Securities Regulation before 1934

Before the creation of the Securities and Exchange Commission (SEC) in 1934, financial markets in the United States were severely under-regulated. Before the

---

[30] J. R. Edwards, *Legal Regulation of British Company Accounts, 1836–1900* (New York: Garland, 1986), 17.
[31] L. R. Dicksee, *Auditing: A Practical Manual for Auditors* (New York: Arno, 1976), 6. Reprint of the 1892 edition.
[32] Id., 1–9.

stock market crash of 1929, there was very little appetite for federal regulation of the securities market, and proposals that the government require financial disclosure and prevent the fraudulent sale of stock were not seriously pursued.[33] Investors were largely unconcerned about the dangers of investing in an unregulated market. In fact, many were seduced by the notion that they could make huge sums of money on the stock market. In the 1920s, approximately 20 million large and small shareholders took advantage of the postwar boom in the economy and tried to make their fortunes by investing in securities.[34]

Although there was little interest during the first decades of the century in instituting federal oversight of the securities industry, state legislatures had already begun to regulate the securities industry.[35] States in the Midwest and West were most active in pursuing securities regulation in response to citizens' complaints that unscrupulous salesmen and dishonest stock schemes were victimizing them.[36] The first comprehensive securities law of the era was enacted by Kansas in 1911. That law, the first of many known as *blue-sky laws,* required the registration of both securities and those who sold them.[37] The intent was to prevent fraud in the sale of securities and also to prevent the sale of securities of companies whose organization, plan of business, or contracts included provisions that were "unfair, unjust, inequitable, or oppressive" or if the investment did not "promise a fair return." In the two years following the enactment of the securities laws in Kansas in 1911, 23 states passed some form of blue-sky legislation.[38]

It was only after the stock market crash in 1929 and the ensuing Great Depression that interest in enacting federal securities legislation became widespread. Congress passed the Securities Act of 1933, which had the basic objectives of requiring that investors receive financial and other significant information concerning securities offered for public sale, and prohibiting deceit, misrepresentations, and other fraud in the sale of securities. The primary means of accomplishing these goals was the disclosure of important financial information through the registration of securities.[39]

The second fundamental set of laws, the Securities Exchange Act of 1934, created the Securities and Exchange Commission and granted it broad authority over all aspects of the securities industry, including registering, regulating, and overseeing brokerage firms, transfer agents, and clearing agencies. The Act addressed the need for regulation of the securities industry, as well as the need to address the potential

[33] U.S. Securities and Exchange Commission, "Introduction—The SEC: Who We Are, What We Do," www.sec.gov.
[34] Id.
[35] Wisconsin Department of Financial Institutions, "A Brief History of Securities Regulation," www.wdfi.org/fi/securities/regexemp/history.htm.
[36] Id.
[37] Id.
[38] Id.
[39] U.S. Securities and Exchange Commission, "Introduction—The SEC: Who We Are, What We Do."

for fraud inherent within it. Several sections of the Act deal with fraud, including Section 9 (Manipulation of Security Prices), Section 10 (Manipulative and Deceptive Devices), Section 18 (Liability for Misleading Statements), Section 20 (Liability of Controlling Persons and Persons Who Aid and Abet Violations), and Section 20A (Liability to Contemporaneous Traders for Insider Trading).

Current Environment

The financial scandals in the years 2000 and 2001 at major corporations and conflict of interest issues in the financial services industry caused investor confidence in the stock market to decline dramatically. In response to the wave of corporate malfeasance, the U.S. Congress passed the Sarbanes-Oxley Act of 2002, intended to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."[40]

Sarbanes-Oxley prohibits accounting firms from providing many consulting services for the companies they audit, requires audit committees to select and essentially oversee the external auditor, and generally strengthens the requirement that auditors must be independent from their clients. Section 101 of the Sarbanes-Oxley Act established the Public Company Accounting Oversight Board (PCAOB) to oversee the audit of public companies that are subject to the securities laws and related matters. The purpose of the PCAOB is to protect the interests of investors and to further the public interest.[41] The PCAOB was authorized to establish auditing and related professional practice standards, and Rule 3100 requires the auditor to comply with these standards.[42] The Sarbanes-Oxley Act began an extensive and still-evolving series of audit rule changes, prompting the issuance of three auditing standards.

In October 2002, the AICPA issued *Statement on Auditing Standards (SAS) No. 99,* "Consideration of Fraud in a Financial Statement Audit." Effective for audits of financial statements for periods beginning on or after December 15, 2002, SAS 99 sought to improve auditing practice, especially as it relates to the auditor's role in detecting fraud, if it exists, in the course of the audit. According to the AICPA president and CEO, the standard was meant to "substantially change auditor performance, thereby improving the likelihood that auditors will detect material misstatements due to fraud" by putting "fraud in the forefront of the auditor's mind."[43] Furthermore, according to the AICPA's own assessment, the standard would be the "cornerstone

---

[40] Sarbanes-Oxley Act of 2002, Public Law 107–204, 107th Cong., 2d sess. (January 23, 2002), 1 (from statute's official title: "An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes").

[41] Public Company Accounting Oversight Board, Sarbanes-Oxley Act of 2002, www.pcaobus.org/rules/Sarbanes_Oxley_Act_of_2002.pdf.

[42] Public Company Accounting Oversight Board, Rules of the Board, 127, www.pcaobus.org/documents/rules_of_the_board/Standards-AS1.pdf.

[43] American Institute of Certified Public Accountants, "AICPA Issues New Audit Standard for Detecting Fraud, Cornerstone of Institute's New Anti-Fraud Program," October 15, 2002, www.aicpa.org/news/2002/p021015.htm.

of a multifaceted effort by the AICPA to help restore investor confidence in U.S. capital markets . . . to reestablish audited financial statements as a clear picture window into Corporate America."[44] The standard, however, does not increase or alter the auditor's fundamental responsibility, which is to plan and conduct an audit such that if there is a fraud or error causing a material misstatement of a company's financial statements, it may be detected. While this seems an unambiguous mandate, there still remains a difference between the public perception that audits should detect all fraud and the actual standards governing the conduct of audits. There is a significant and legitimate difference between *performing an audit* and *conducting a financial fraud investigation*. That difference is explored throughout this book.

In November 2003, the SEC approved the final versions of corporate governance listing standards proposed by the NYSE and NASDAQ stock markets. Both standards expand upon the Sarbanes-Oxley Act of 2002 and SEC rules to impose significant new requirements on listed companies. These sweeping reforms mandate independence of directors, increased transparency, and new standards for corporate accountability. These and other governance standards emphasize the importance of enhancing governance, ethics, risk, and compliance oversight capabilities.

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its new Enterprise Risk Management framework. The new COSO framework identifies key elements of an effective enterprise risk management approach for achieving financial, operational, compliance, and reporting objectives. The new COSO framework emphasizes the critical role played by governance, ethics, risk, and compliance in enterprise management.

On November 1, 2004, the United States Organizational Sentencing Guidelines (the Guidelines) were amended to provide expanded guidance regarding the criteria for effective compliance programs. The Guidelines emphasize the importance of creating a "culture of compliance" within the organization; establish the governance and oversight responsibilities of the board and senior management; and frame the need for dedicating appropriate resources and authority. The Guidelines also focus on the relationship between governance, ethics, risk management, and compliance.

These efforts, though laudable, have not prevented a further wave of financial market turmoil. The collapse of the credit markets in the United States and Europe was brought on in part by the bursting real estate bubble and the consequent exposure of poor lending practices as financial institutions chased fee income from generating new transactions, instead of traditional sources of profitability based on their interest rate spread between assets and liabilities. At the same time, the rise of unregulated private equity, hedge fund, and other investment partnerships promising returns beyond market expectations in size and stability fueled speculative investing and poor due diligence practices. The failure during this liquidity crisis of massive financial market participants like Countrywide and Merrill Lynch (both absorbed by Bank of America), Bear Stearns being merged with JP Morgan Chase, Lehman Brothers falling into liquidation, and Citigroup and AIG, among others, receiving billions in government support payments (see Exhibit 1.1) has been the consequence of speculation in the markets.

[44] Id.

EXHIBIT 1.1 Largest Recipients of TARP: Capital Purchase Program[45]

Date	Institution	Amount
10/28/2008	Wells Fargo and Company	$25,000,000,000
10/28/2008	JP Morgan Chase and Co.	$25,000,000,000
10/28/2008	Citigroup, Inc.	$25,000,000,000
10/28/2008	Bank of America Corporation	$15,000,000,000
10/28/2008	The Goldman Sachs Group, Inc.	$10,000,000,000
10/28/2008	Morgan Stanley	$10,000,000,000
1/9/2009	Bank of America Corporation	$10,000,000,000

This volatile combination of investor greed and institutional focus on transaction flow as opposed to credit risk management has spawned a new wave of investor and market protection regulation. Most significant among these newly proposed measures is the proposal (pending at the time this chapter was written) to establish a new oversight agency called the Consumer Financial Protection Agency. Legislation proposed by President Obama's administration in 2009 calls for the establishment of an agency that will be charged with setting and enforcing clear rules for consumers and banks. The SEC is also taking aim at improving their expertise and efficiency through various initiatives, including creating five new national specialized investigative groups dedicated to high priority areas of enforcement (that is, asset management, market abuse, structured and new products, the Bureau of Consumer Financial Protection, and municipal securities).[46] Despite the experiences from the burst of the dotcom bubble in 2000 and 2001, it appears that financial markets and financial market participants remained a step ahead of regulations, demonstrating that fraud is a continuing and intractable problem, to which many lend substantial creative energy, as is discussed in Chapter 2, "Psychology of the Fraudster."

Other significant developments are attempts at increased transparency relating to corporate risk management and compensation practices, as well as calls for significant pay regulation of top executives, especially at entities funded in part by government money. Effective February 28, 2010, SEC rules require disclosure in proxy and information statements to include:

- The relationship of a company's compensation policies and practices to risk management
- The background and qualifications of directors and nominees
- Legal actions involving a company's executive officers, directors, and nominees
- The consideration of diversity in the process by which candidates for director are considered for nomination

[45] http://financialstability.gov/docs/transaction-reports/3-26-10 Transactions Report as of 3-24-10.pdf.

[46] December 8, 2009, speech by Robert Khuzami, director, Division of Enforcement, SEC staff: Remarks at AICPA National Conference on Current SEC and PCAOB Developments. www.sec.gov.

- Board leadership structure and the board's role in risk oversight
- Stock and option awards to company executives and directors
- Potential conflicts of interest of compensation consultants[47]

The United Kingdom has acted similarly in this period, proposing a tax on executive bonus of 50 percent on amounts over 25,000 pounds.

Much of this regulatory activity was in response to the fraudulent mortgage origination practices in the U.S. real estate industry. Consistently rising housing prices in many parts of the nation, combined with new financial products and a banking industry that treated mortgages as a *fee-flow* and an asset to be *securitized* and sold off to others, and the uniquely irresponsible American approach to credit consumption to "keep up with the Joneses" created fertile grounds for fraud. One popular mortgage product—the no-documentation loan—went so far as to encourage fraudulent misrepresentation of assets or income by eliminating the documentation requirements.

On the corporate finance front, the basic principles of a fraudulent borrowing scheme were alleged against issuers and brokers of *auction rate securities*. These short-term corporate finance vehicles, similar to commercial paper, were allegedly sold to investors on the basis of their cash-like security, but with a higher return. The safety of the investor's money, however, depended entirely upon the sufficiency of bidders at each auction date, at which time the interest rate for the coming period was set. Without sufficient bidders, an investor looking to withdraw his funds could not, and was forced to reinvest. The attorney general of the state of New York brought several successful actions alleging various financial institutions made misrepresentations in their marketing and sales of auction rate securities that were marketed and sold as safe, cash-equivalent products, when in fact they faced increasing liquidity risk.[48] Several firms, including Merrill Lynch, Goldman Sachs, Deutsche Bank, and Wachovia reached settlements with the attorney general in which the firms agreed to buy-backs of all auction rate securities. In the case against Wachovia,[49] Wachovia represented to its customers that auction rate securities were "money market alternatives" and "liquid investments," when in fact auction rate securities were different from cash and money market instruments because the liquidity of the auction rate security relied on the successful operation of the auction. According to the attorney general, investors relied upon these representations, and when the market collapsed in February 2008, investors were stuck holding on to securities with no value.

AUDITORS ARE NOT ALONE

Although auditors have long been recognized to have an important role in detecting fraud, it is well recognized that they do not operate in a vacuum. Management,

[47] December 16, 2009, "SEC Approves Enhanced Disclosure about Risk, Compensation and Corporate Governance," www.sec.gov.
[48] www.ag.ny.gov/media_center/2009/feb/feb5c_09.html.
[49] Attorney General of the State of New York Investor Protection Bureau in the matter of Wachovia Securities, LLC, and Wachovia Capital Markets, LLC, according to the Wachovia settlement.

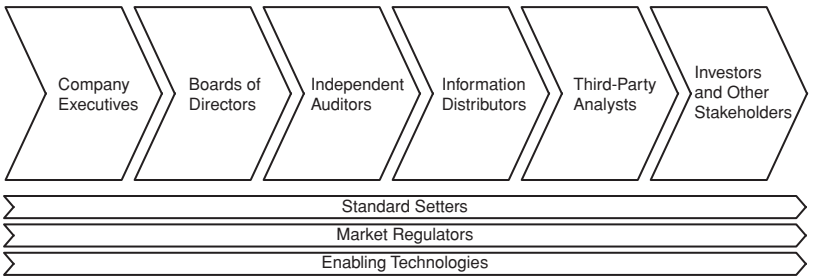


EXHIBIT 1.2 The Corporate Reporting Supply Chain

boards of directors, standard setters, and market regulators are key participants in corporate governance, each charged with specific responsibilities in the process of ensuring that financial markets, investors, and other users of corporate financial reports are well served. They are, in effect, links in a corporate reporting supply chain (CRSC) that includes several additional participants (see Exhibit 1.2).

The concept of the corporate reporting supply chain makes clear that auditors are only one of several interconnected participants having a role in delivering accurate, timely, and relevant financial reports into the public domain.[50] While many may consider the internal, external, and regulatory auditors as the first lines of defense against fraud, they are, in fact, all in secondary positions. The first line of defense is a properly constructed system of corporate governance, risk management, and internal controls, for which management is responsible. The board, in turn, and its audit committee are responsible for overseeing management on behalf of shareholders, and so the board, too, has its share of responsibility for defending against fraud.

Management and the board share responsibility for certain critical aspects of deterring fraud in financial reporting:

- Setting a "tone at the top" that communicates the expectation of transparent and accurate financial reporting
- Responding quickly, equitably, and proportionately to violations of corporate policy and procedure
- Maintaining internal and external auditing processes independent of management's influence
- Ensuring a proper flow of critical information to the board and external parties
- Establishing an adequate system of internal accounting control that will satisfy the requirements of Section 404 of the Sarbanes-Oxley Act
- Investigating and remediating problems when they arise

These duties are far-reaching. They incorporate responsibilities from every component of the fraud deterrence cycle discussed in the next section. And they represent

[50] Samuel A. DiPiazza and Robert G. Eccles, *Building Public Trust: The Future of Corporate Reporting* (Hoboken, NJ: John Wiley & Sons, 2002), 10–11, 43. This is a principal focus of PCAOB Auditing Standard No. 2 (AS2).

the first line of defense against fraud. While an audit responds to the risk of fraud, the forensic accounting investigation responds to suspicions, allegations, or evidence of fraud. These different activities are explored throughout this text.

DETERRENCE, AUDITING, AND INVESTIGATION

The increased size and impact of financial reporting scandals and the related loss of billions of dollars of shareholder value have rightly focused both public and regulatory attention on all aspects of financial reporting fraud and corporate governance. Some of the issues upsetting investors and regulators—for example, executive pay that could be considered by some to be excessive—are in the nature of questionable judgments, but do not necessarily constitute fraud. At the other end of the spectrum, there have been more than a few examples of willful deception directed toward the investing community through fabricated financial statements, and many of these actions are being identified and punished—for example, Bernie Madoff's audacious Ponzi scheme. The investing public may not always make a fine distinction between the outrageous and the fraudulent—between bad judgment and wrongdoing. However, for professionals charged with the deterrence, discovery, investigation, and remediation of these situations, a systematic and rigorous approach is essential.

The remainder of this chapter discusses various elements of what we call the *fraud deterrence cycle* (Exhibit 1.3), many of which will be the topics of chapters to come. Without an effective regimen of this kind, fraud is much more likely to occur. Yet even with a fraud deterrence regimen effectively in place, there remains a chance that fraud will occur. Absolute fraud prevention is a laudable but unobtainable goal. No one can create an absolutely insurmountable barrier against fraud, but many sensible precautionary steps can and should be taken by organizations to deter

EXHIBIT 1.3 The Fraud Deterrence Cycle

fraudsters and would-be fraudsters. While fraud cannot be completely prevented, it can and should be deterred.

CONCEPTUAL OVERVIEW OF THE FRAUD DETERRENCE CYCLE

The fraud deterrence cycle occurs over time, and it is an interactive process. Broadly speaking, it has four main elements:

1. Establishment of corporate governance and risk assessment
2. Implementation of transaction-level control processes, often referred to as the system of internal accounting controls; generally of both a deterrent (often called *preventative*) and detective nature
3. Retrospective examination of governance and control processes through audit examinations
4. Investigation and remediation of suspected or alleged problems

Corporate Governance

An appropriate system of governance should be born with the company itself, and grow in complexity and reach as the company grows. It should predate any possible opportunity for fraud. Corporate governance is about setting and monitoring objectives, tone, policies, risk appetite, accountability, and performance. Embodied in this definition is also a set of attitudes, policies, procedures, delegations of authority, and controls that communicate to all constituencies, including senior management, that fraud will not be tolerated. It further communicates that compliance with laws, ethical business practices, accounting principles, and corporate policies is expected, and that any attempted or actual fraud is expected to be disclosed by those who know or suspect that fraud has occurred. There is substantial legal guidance concerning standards for corporate governance, but generally, the substance and also the vigorous communication of governance policies and controls need to make clear that fraud will be detected and punished. While prevention would be a desirable outcome for corporate governance programs, complete prevention is impossible. Deterrence, therefore, offers a more realistic view. In short, corporate governance is an entire culture that sets and monitors behavioral expectations intended to deter the fraudster.

Today, changes in business are being driven by increased stakeholder demands, heightened public scrutiny, and new performance expectations. Critical issues related to governance reform are surfacing in the marketplace on a daily basis. These issues include:

- Protecting corporate reputation and brand value
- Meeting increased demands and expectations of investors, legislators, regulators, customers, employees, analysts, consumers, and other stakeholders
- Searching for new markets and growth in an increasingly interconnected global economy

- Driving value and managing performance expectations for governance, ethics, risk management, and compliance
- Managing crisis and remediation while defending the organization and its executives and board members against the increased scope of legal enforcement and the rising impact of fines, penalties, and business disruption

Boards and management must effectively oversee a number of key business processes to better execute effective governance, including the following:

- Strategy and operational planning
- Risk management
- Ethics and compliance (tone at the top)
- Performance measurement and monitoring
- Mergers, acquisitions, and other transformational transactions
- Management evaluation, compensation, and succession planning
- Communication and reporting
- Governance dynamics

All the preceding elements are critical to a good governance process.

Transaction-Level Controls[51]

Transaction-level controls are next in the cycle. They are accounting and financial controls designed to help ensure that only valid, authorized, and legitimate transactions occur and to safeguard corporate assets from loss due to theft or other fraudulent activity. These procedures are preventive because they may actively block or prevent a fraudulent transaction from occurring. Such systems, however, are not foolproof, and fraudsters frequently take advantage of loopholes, inconsistencies, or vulnerable employees. As well, they may engage in a variety of deceptive practices to defeat or deceive such controls. Anti-money-laundering procedures employed by financial institutions are an excellent example of a proactive process designed to deter fraudulent transactions from taking place through a financial institution. Another familiar example is policy relating to the review and approval of documentation in support of disbursements.

Retrospective Examination

The first two elements of the fraud deterrence cycle are the first lines of defense against fraud and are designed to deter fraud from occurring in the first place. Next in the cycle are the retrospective procedures designed to help detect fraud before it becomes large and, consequently, harmful to the organization. Retrospective procedures such as those performed by management, auditors, and forensic accounting investigators do not prevent fraud in the same way that front-end transaction controls do, but they form a key link in communicating intolerance for fraud and discovering problems

[51] Principal focus of PCAOB Auditing Standard No. 2 (AS2).

before they grow to a size that could threaten the welfare of the organization. Furthermore, with the benefit of hindsight, the cumulative impact of what may have appeared as innocent individual transactions at the time of execution may prove to be problematic in the aggregate. Although detective controls and auditing cannot truly prevent fraud in the sense of stopping it before it happens, they are an important part of an overall fraud deterrence regime.

Investigation and Remediation

Positioned last in the fraud deterrence cycle is forensic accounting investigation of suspected, alleged, or actual frauds. Entities that suspect or experience a fraud should undertake a series of steps to credibly maintain and support the other elements of the fraud deterrence cycle. Investigative findings often form the basis for both internal actions such as suspension or dismissal and external actions[52] against the guilty parties or restatement of previously issued financial statements. An investigation should also form the basis for remediating control procedures. Investigations should lead to actions commensurate with the size and seriousness of the impropriety or fraud, no matter whether it is found to be a minor infraction of corporate policy or a major scheme to create fraudulent financial statements or misappropriate significant assets.

All elements of the cycle are interactive. Policies are constantly reinforced and revised, controls are continually improved, audits are regularly conducted, and investigations are completed and acted upon as necessary. Without the commitment to each element of the fraud deterrence cycle, the overall deterrent effect is substantially diminished.

FIRST LOOK INSIDE THE FRAUD DETERRENCE CYCLE

We have seen that the fraud deterrence cycle involves four elements: corporate governance, transaction-level controls, retrospective examination, and investigation and remediation. Here we want to take a first look inside each of the elements to identify some of their main features.

Corporate Governance

In our experience, the key elements of corporate governance are:

- An independent board composed of a majority of directors who have no material relationship with the company
- An independent chairperson of the board *or* an independent lead director
- An audit committee that actively maintains relationships with internal and external auditors
- An audit committee that includes at least one member who has financial expertise, with all members being financially literate

[52] See Chapter 19 for considerations surrounding a referral of matters for prosecution.

- An audit committee that has the authority to retain its own advisors and launch investigations as it deems necessary
- Nominating and compensation committees composed of independent directors
- A compensation committee that understands whether it provides particularly lucrative incentives that may encourage improper financial reporting practices or other behavior that goes near or over the line
- Board and committee meetings regularly held without management and CEO present
- Explicit ethical commitment ("walking the talk") and a tone at the top that reflects integrity in all respects
- Prompt and appropriate investigation of alleged improprieties
- Internally publicized enforcement of policies on a no-exception or zero-tolerance basis
- The board or audit committee's reinforcement of the importance of consistent disciplinary action of individuals found to have committed fraud
- Timely and balanced disclosure of material events concerning the company
- A properly administered hotline or other reporting channels, independent of management
- An internal audit function that reports directly to the audit committee without fear of being "edited" by management (CEO, CFO, controller, and others)
- Budgeting and forecasting controls
- Clear and formal policies and procedures, updated in a timely manner as needed
- Well-defined financial approval authorities and limits
- Timely and complete information flow to the board

Transaction-Level Controls

Systems of internal accounting control are also key elements in the fraud deterrence cycle. Literature on this topic is extensive, but one manual in particular is widely recognized as authoritative: *Internal Control—Integrated Framework*, prepared by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and published by the American Institute of Certified Public Accountants. This manual lays out a comprehensive framework for internal control. Any entity undertaking fraud deterrence will want to be conversant with the elements and procedures covered in this book. Briefly, the critical elements highlighted in the COSO framework are:

- *The Control Environment.* This is the foundation for all other components of internal control, providing discipline and structure, and influencing the control awareness of the organization's personnel. Control environment factors include the integrity, ethical values, and competence of the organization's people; management's philosophy and operating style; management's approach to assigning authority and responsibility; and how personnel are organized and developed.[53]

[53] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework* (New York: Committee of Sponsoring Organizations of the Treadway Commission, 1994), 23. Note: Commonly referred to as the COSO Report.

- *Risk Assessment*. Effectively assessing risk requires the identification and analysis of risks relevant to the achievement of the entity's objectives as a basis for determining how those risks should be managed and controlled. Because economic, industry, regulatory, and operating conditions continually change, mechanisms are needed to identify and deal with risks on an ongoing basis.[54]
- *Control Activities*. Control activities occur throughout an organization at all levels and in all functions, helping to ensure that policies, procedures, and other management directives are carried out. They help, as well, to ensure that necessary actions are taken to address risks that may prevent the achievement of the organization's objectives. Control activities are diverse, but certainly may include approvals, authorizations, verifications, reconciliations, operating performance reviews, security procedures over facilities and personnel, and segregation of duties.[55]
- *Information and Communication*. Successfully operating and controlling a business usually requires the preparation and communication of relevant and timely information. This function relies in part on information systems that produce reports containing operational, financial, and compliance-related data necessary for informed decision making. Communication should also occur in the broader sense, flowing down, up, and across the organization, so that employees understand their own roles and how they relate to others. Furthermore, there must be robust communication with external parties such as customers, suppliers, regulators, and investors and other stakeholders.[56]
- *Monitoring*. COSO recognizes that no system can be both successful and static. It should be monitored and evaluated for improvements and changes made necessary by changing conditions. The scope and frequency of evaluations of the internal control structure depend on risk assessments and the overall perceived effectiveness of internal controls. However, under the Sarbanes-Oxley requirements, management and the external auditors are each charged with performing an evaluation at least annually.[57]

To serve the needs of a thorough fraud deterrence cycle, several aspects of control processes are of particular importance. Among them are the following:

- Additions, changes, or deletions to master data files of customers, vendors, and employees
- Disbursement approval processes
- Write-off approval processes (in accounts such as bad debt, inventory, and so forth)
- Revenue recognition procedures
- Inventory controls

[54] Id., 33.
[55] Id., 49.
[56] Id., 59.
[57] Id., 69.

- Processes for signing contracts and other agreements
- Segregation of duties
- Information systems access and security controls
- Proper employment screening procedures, including background checks
- Timely reconciliation of accounts to subsidiary ledgers or underlying records
- Cash management controls
- Safeguarding of intellectual assets such as formulas, product specifications, customer lists, pricing, and so forth
- Top-level reviews of actual performance versus budgets, forecasts, prior periods, and competitors

AUDITING AND INVESTIGATION

The remaining two elements of the fraud deterrence cycle are retrospective examination, that is, auditing and investigation, and remediation of any discovered problems. As discussed later in detail, there are differences between auditing and investigating.

	GAAS Audit	Forensic Accounting Investigation
Objective	Form an opinion on the overall financial statements taken as a whole	Determine the likelihood or magnitude of fraud occurring[a]
Purpose	Usually required by third-party users of financial statements	Sufficient predication that a fraud has or may have occurred
Value	Adds credibility to reported financial information	Resolves suspicions and accusations; determines the facts
Sources of evidence	Inquiry, observation, examination, and reperformance of accounting transactions to support financial statement assertions	Review detailed financial and nonfinancial data, search public records, conduct fact-finding as well as admission-seeking interviews, including third-party inquiries
Sufficiency of evidence	Reasonable assurance	Establish facts to support or refute suspicions or accusations

[a]Ultimately the trier of fact concludes whether fraud has occurred. The focus of a fraud investigation is fact finding, based on the investigator's knowledge of the elements of fraud that a trier of fact considers.
Source: Adapted from Association of Certified Fraud Examiners.

These differences make clear that audits and investigations are not the same. During the course of an audit, an auditor seeks to detect errors or improprieties, absent any specific information that such improprieties exist. During an investigation, a forensic accounting investigator seeks to discover the full methods and extent of improprieties that are suspected or known. Both are important features of the fraud deterrence cycle, but they are, and should be, separate. They involve different

procedures and they are performed by professionals with different skills, training, education, knowledge, and experience. This is an important distinction in the current environment, when some commentators have suggested that the spate of corporate scandals cries out for the conversion of the financial statement audit into something resembling an investigation. If an audit in the future were to take this path, the cost of performing audits would most likely increase.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 2

Psychology of the Fraudster

Thomas W. Golden

Start with the pleasant assumption that most people are honest. It's a nice way to look at the world, and it summons up childhood memories about learning that honesty is the best policy and George Washington telling his father, "I cannot tell a lie."

Sad to say, human history and human nature tell a different story, and so do the statistics that examine them. While most societies explicitly abhor violent crime and bodily harm, many societies hold financial fraud, whatever its scale, as a less reprehensible wrongdoing. Charles Ponzi, creator of the Ponzi scheme, was celebrated in some quarters as a folk hero and cheered by many of the people he helped to defraud. Financiers and executives, whose frauds can disrupt thousands or tens of thousands of lives, have historically been punished with relatively light sentences or serve their time at a low-security federal "tennis camp." Some scholars have called this attitude toward white collar crime "a perversion of our general societal admiration for intelligence."[1] With the advent of the Sarbanes-Oxley Act in 2002 and recent increases in prison terms for certain financial crimes, there is the expectation that this perception will change and white collar criminals will begin to endure what many would deem just punishment for their crimes.

During much of the past century, psychologists and sociologists struggled to understand the inner workings of people who commit white collar crime. Edwin Sutherland's *White Collar Crime,*[2] the most influential work in the field, argued in 1939 that an individual's personality has no relevance to a propensity to commit such crimes. Rather, he said, economic crimes originate from the situations and social bonds within an organization, not from the biological and psychological characteristics of the individual.[3] Sutherland also made the useful, if apparent, observation that criminality is not confined to the lower classes and to social misfits but extends, especially where financial fraud is concerned, to upper-class, socially well-adjusted people. Later authors introduced quite different ideas—for example, suggesting that

[1] Ezra Stotland, "White Collar Criminals," *Journal of Social Issues* 33(4) (1977): 179–196. The author offers a detailed discussion of society's ambivalent attitude toward certain white collar criminals.
[2] Edwin H. Sutherland, *White Collar Crime* (New Haven, CT: Yale University Press, 1983), 7.
[3] Id.

financial fraud is an inevitable feature of capitalism, in which the culture of competition promotes and justifies the pursuit of material self-interest, often at the expense of others and even in violation of the law.[4]

Over the many decades since *White Collar Crime* was published, persuasive studies have argued that two factors should be considered in analyzing the psychology and personality of the fraudster:

- The biological qualities of an individual, which vary widely and influence behavior, including social behavior
- The social qualities that are derived from and in turn shape how the individual deals with other people[5]

From these studies of psychology, two general types of financial fraudster have been observed:

- Calculating criminals who want to compete and to assert themselves
- Situation-dependent criminals who are desperate to save themselves, their families, or their companies from a catastrophe[6]

Since these studies were published, a third type of criminal has emerged out of catastrophic business failures and embarrassments. We call them *power brokers*.

CALCULATING CRIMINALS

Calculating criminals are predators. They tend to be repeat offenders, they have higher-than-average intelligence, and they're relatively well educated. They usually begin their careers in crime later in life than other criminals.[7] These predators are generally inclined to risk taking—no surprise there—and they lack feelings of anxiety and empathy.[8] A related view, somewhat different in its emphasis, was offered in a 1993 study of Wall Street's insider-trading scandals by a team of psychologists who suggested that individuals willing to commit such crimes had an "external locus of control"—that is, they lacked inner direction, self-confidence, and self-esteem and were motivated by their desire to fit in and be accepted. Furthermore, the study found that they define success by others' standards.[9]

---

[4] James E. Coleman, "Toward an Integrated Theory of White-Collar Crime," *American Journal of Sociology* 93 (1987): 406–439.
[5] R. Lazarus, *Personality* (Stockholm: Wahlström and Widstrand, 1973), 12–13.
[6] These categories and the research supporting them are discussed in detail by Tage Alalehto, "Economic Crime: Does Personality Matter?" *International Journal of Offender Therapy and Comparative Criminology* 47(3) (2003): 335–355.
[7] David Weisbrod, Ellen F. Chayet, and Eljin J. Waring, "White-Collar Crime and Criminal Careers: Some Preliminary Findings," *Crime and Delinquency* 36(3) (1990): 342–355.
[8] Georges Kellens, "Sociological and Psychological Aspects," *Criminological Aspects of Economic Crime* 15 (Strasbourg, France: European Committee on Crime Problems, 1977).
[9] D. E. Terpstra, E.J. Rozel, and P.K. Robinson, "The Influence of Personality and Demographic Variables on Ethical Decisions Related to Insider Trading," *Journal of Psychology* 127(4) (1993): 375–389.

Case 1: "It Can't Be Bob"

Bob Davies (not his real name) seemed to be a terrific employee as vice president of operations at a billion-dollar company that he had joined six years before. His résumé listed academic and business successes. He was well liked and a hard worker, always willing to pitch in and help break a logjam. When needed, he worked nights or weekends—whatever it took to get the job done. He remembered employees' names, used them when giving out praise, and, even remembering their children's names, would often ask about their children. Then, one day, Davies wired $10 million of his company's money to a bank in Germany and took off after it, bringing along his secretary and abandoning his wife of 12 years and their three children.

"There must be some mistake. It can't be Bob," echoed through the office. To Davies's friends and colleagues, this episode was a nightmare. To the forensic accounting investigators called in to investigate, the incident was in its main features unsurprising. Appearances notwithstanding, Davies was a predator—a con man whose life's work was to steal for personal gain. Predators develop considerable skills and make a career of deceiving people, as though it were just another career track to follow. Predators are dangerous and cause great harm. And once in place, they're hard to detect. The chances are good that a predator who wants access to company assets will accomplish that goal regardless of the controls established to prevent intrusion. Fraud deterrence and detection controls are often robust enough to stop other types of white collar criminals, but they may not stop the predator. The best defense against predators—somewhat sadly and disturbingly—is a thorough background check *before hiring*. This is a key element of an antifraud program. The company that employed Davies could have discovered his four prior felony convictions during the hiring process. If it had, he wouldn't have been hired.

SITUATION-DEPENDENT CRIMINALS

The vast majority of corporate criminals, however, are not predators at all. They are situation-dependent criminals: seemingly ordinary people who commit crimes without the intent to harm others. This is a key to understanding white collar crime, because almost all news coverage and much of the scholarly literature in the area focuses on "egregious, highly publicized, and largely atypical cases" and ignores "the more common, run-of-the-mill, garden-variety" offenders and offenses that account for most white collar crimes.[10]

This category of financial fraudster—run of the mill, garden variety, but still capable of doing great harm—is the focus of the balance of this chapter.

The white collar criminals profiled in Exhibit 2.1 don't stand out. Many employees share these characteristics.

At the start of an investigation, the forensic accounting investigator often sits down with the client and goes over the organizational chart. The forensic accounting investigator and the client talk about each employee one by one, about each employee's work, and about what is known of the lifestyle of each.

[10] Michael L. Benson and Elizabeth Moore, "Are White-Collar and Common Offenders the Same? An Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime," *Journal of Research in Crime and Delinquency* 29(3) (1992): 251–272.

EXHIBIT 2.1 Characteristics of the Typical White Collar Criminal

Typical White Collar Criminal
- Older (30-plus years)
- 55 percent male, 45 percent female
- An appearance of a stable family situation
- Above-average (postgraduate) education
- Less likely to have criminal record
- Good psychological health
- Position of trust
- Detailed knowledge of accounting systems and their weaknesses
- Prior accounting experience

Source: Association of Certified Fraud Examiners.

"What about Anne?" the forensic accounting investigator might say, pointing to an employee on the chart. "Oh, no, it couldn't be Anne. She's been with us for 20 years," the client responds. "She's always assisting others with their duties. She's pleasant and rarely takes time off. My wife and I have been to her home. Our daughters are on the same soccer team." The client may believe that what he knows, or thinks he knows, about Anne's character eliminates her from the list of suspects of fraud. In fact, an experienced forensic accounting investigator will understand that Anne fits the profile of a white collar criminal. This is not to suggest that all nice people are criminals but, rather, that most white collar criminals give the appearance of being nice people, thereby fitting the exact profile of Anne.

POWER BROKERS

Many of today's once highly placed corporate criminals show characteristics of each of the previous two categories, but they are different enough in their methods and motives to deserve a category all their own: power brokers. Like many of us, you have read about their excesses and asked yourself how respected business leaders could have been so deluded as to believe that they could usurp the financial and human resources of their companies to line their own pockets and deceive a wide range of stakeholders, including their own employees.

Do the U.S. corporate leaders who face criminal charges begin their careers with the intention of creating a company that would enrich themselves while eventually destroying the dreams and plans of thousands of innocent victims—employees and investors alike? Are any of them predators? Probably not. But a combination of predator characteristics and the circumstances of their positions could lead them to commit financial crimes.

FRAUDSTERS DO NOT INTEND TO HARM

Generally speaking, situation-dependent criminals carry out their frauds with no intention to do any harm. A high-ranking executive of the Westinghouse Electric

Company who was accused of price-fixing in 1961 was asked whether he thought his behavior was illegal. He responded: "Illegal? Yes, but not criminal. Criminal action means hurting someone, and we did not do that."[11]

It is critical to an understanding of the psychology of such people to accept this key point: Most of them carry out their frauds with no intention of doing harm, and they believe—they are able to convince themselves—that what they're doing is not wrong. These people may even convince themselves that what they're doing is for the good of the company and everyone associated with it, including employees, investors, creditors, and other constituencies. Or they may believe that they deserve the spoils they seize because they rationalize their crimes as immaterial, innocent, or deserved—but not *wrong*. In most cases, they start small, but in time the fraud grows in size, usually encompassing more than one scheme.

Case 2: "For the Good of the Company"

The duping effect of rationalization can be carried to an extreme. In an investigation of a public company's chief financial officer (CFO), placed on administrative leave during the investigation, the independent counsel hired by the company said, "He was trying to help the company, but his misguided efforts just ended up getting him as well as the company in trouble." When asked exactly what he meant by good intentions, the counsel said, "What he did he did for the good of the company." The CFO was found guilty of participating in a fraud, and the company paid a fine of $8 million. Thus, rather than "helping out the company," the CFO caused the company to incur significant penalties. The CFO's motivation: getting great discounts from the vendor for his company.

Case 3: Personal Catastrophes

White collar criminals are difficult to spot. A 45-year-old middle manager at a textile manufacturer, making $85,000 a year, gets laid off after his company has become weakened by global competition. He held no one responsible; his only concern was to find another suitable job quickly, before his savings ran out. But he couldn't find one for 14 months, and when he did, it wasn't what he had hoped for. Still, he didn't have to relocate his family, and he did have a managerial position with some prospects for promotion in the next several years. Then the dreadful news began piling up.

His little girl hadn't seen the jagged sidewalk that her bicycle wheel slammed into, throwing her over the handlebars. At the hospital, the doctor assured him that his daughter was in no danger and that a good plastic surgeon could restore her features. But the family's HMO ruled that the procedures were cosmetic and that a substantial portion of the expense would not be covered. Then his mother-in-law had a stroke and needed full-time care. The family had no money for this, so she would have to move in with them. But where? His wife was pregnant with their

[11] Gilbert Geis, "Toward a Delineation of White Collar Offense," *Sociological Inquiry* 32 (1962): 160–171.

second child. No extra bedroom was available for her mother; they would have to build an addition.

The pressure mounted daily. In these circumstances, this harried middle manager was the perfect candidate to become a white collar criminal. He had a *need* and could probably find the *opportunity* to convert some company assets for personal use. All he needed was a way to *rationalize* his actions.

Such circumstances happen every day. Industries contract, high-flying companies taper off, wages and benefits get cut. Surveys have found that for the first time in decades, parents no longer expect their children to have a better life than they do. Under this duress, many people may find that their customary ethical behavior may seem beside the point when criminal opportunities seemingly provide solutions to complex personal problems.[12]

Case 4: An Educated, Upstanding Citizen

We present this case at some length because it touches on many elements in the psychology of the fraudster: the profile of good citizenship, even professional engagement in good works and church affairs, combined with hidden wrongdoing. The case also offers a good introductory example of the forensic accounting investigative team at work.

The board of a Midwestern foundation dedicated to helping Eastern European and Russian children in need of medical assistance asked for a review of its controls over receipts and expenses. A forensic team examining the executive director's expenses noticed that some personal expenses had been charged to the foundation, including $315 for schoolbooks recently purchased for her children. The team expanded the review to an entire year and found evidence that car repairs, groceries, liquor, theater tickets, and a flight to Miami by the director and her family had been paid for by the foundation. The forensic accounting investigators showed the evidence to the board chairman, who was puzzled and who assured the team that the board had not authorized these expenditures. The board then authorized a broader investigation. The question on everyone's mind was: Were these simply clerical errors, misunderstandings—or the work of a dishonest executive director?

Throughout the investigation, the forensic accounting investigators stayed in continual contact with the executive director to give her the impression that she was leading the investigation and had nothing to fear. The forensic accounting investigators were surprised that she might be a fraudster; she did not fit the preconceived profile of the white collar criminal they had in their heads.

Eventually, the investigation determined that the foundation had been paying the private school tuition of the executive director's children, bringing the total of unauthorized expenses to at least $90,000. With no remaining doubt that they had identified a fraudster in the organization, the team now needed to determine whether there might be other fraudulent schemes or coconspirators. Only more investigative work would provide the answers. The Association of Certified Fraud Examiners

[12] Benson and Moore, 262.

(ACFE) fraud manual[13] instructs that once a fraudster has been identified, forensic accounting investigators should:

- Look for additional schemes
- Look for co-conspirators
- Look to see what the targets have touched and test those areas[14]

Having thoroughly examined the director's expenses, the forensic accounting investigators thought about what other possibilities for fraud existed. They learned that the director had been directly involved in conducting fund-raising, and so they needed to track the donations received. This search for possibly unrecognized revenue would prove to be an especially challenging task. The director could easily have converted contributions to the foundation for her personal use without anyone's knowing about it. It would be very difficult indeed to confirm revenue from donors known only to her.

Knowing where to look is greatly facilitated by understanding the operations of the organization and the scope of transactions that a suspect has generated or approved. The forensic team knew that the director favored churches as targets for fund-raising. A good place to start was with a study of her travel around the country, based on her expense report vouchers and correlated with churches near the hotels where she stayed. Each time that the forensic accounting investigators identified a church where she had conducted an appeal, they looked for a deposit in the foundation's bank account. They then began calling each church to track donations. They did not disclose that they were investigating suspected criminal behavior—only that they were auditing the foundation's books and confirming donations. If the response was that a donation had not been made and in fact no such appeal had taken place, the forensic accounting investigators simply apologized for troubling that church.

Before long, they found what they were looking for. At a Presbyterian church in Dallas, the minister told the forensic accounting investigators that the executive director had addressed the congregation one Sunday morning and was handed a check for $10,000: A combination of donations from worshippers and a contribution from the church's discretionary fund authorized by the minister himself. The forensic accounting investigators requested a copy of the check, front and back, and the minister faxed it promptly. They noted the absence of any endorsement—only the handwritten account number of an account different from the foundation's but matching the executive director's personal account number. Here was another fraud

[13] Association of Certified Fraud Examiners, *Fraud Examiners Manual* (Austin, TX: Association of Certified Fraud Examiners, 1998).

[14] For the auditors of this organization, findings of this type present the complex issue of continued reliance on the representations of the executive director. A review of the working papers would likely find specific representations by the executive director, obtained in the course of the audit, as well as her signature on the management representation letter provided to the auditors at or near completion of their work. While another officer might be able to step in and provide the necessary representations, this is often a difficulty cured only through a combination of additional procedures.

scheme in addition to the false reporting of expenses. There was no firm means of determining how many appeals the director had made in the three years of her directorship or how much she had stolen. Without a court order, the forensic accounting investigators could not obtain her personal banking records, although a good investigative procedure in determining possible theft is to determine valid sources for all deposits on a bank statement. The minister mentioned that the appeal had been videotaped, and he provided the team with a copy.

The team now brought its findings to the foundation's board:

- The executive director had stolen at least $90,000 through expense reimbursement and fraudulent payments for personal expenses.
- She had diverted to her own use checks made payable to the foundation and intended for support of its programs.
- The team had been unable to determine how many foundation donations she had diverted.
- The target was not aware that forensic accounting investigators knew of her frauds.

Board members were stunned and not yet ready to take the matter to the prosecutor. "There has to be a reasonable explanation for these allegations," some board members said. Others were worried about the adverse publicity that a criminal prosecution would bring in addition to its effect on their reputations and the future of the foundation.

As the next step, the forensic accounting investigators prepared for an admission-seeking interview (see Chapter 16) in an attempt to get the executive director to admit to the thefts. During that interview, they would also attempt to get the suspect to admit to other frauds or to provide access to her banking records. Eventually, she confessed. Her explanation? "I only borrowed the money and had every intention of paying it back." She rationalized her actions by reasoning that if she could circulate in high society, she'd be in a better position to solicit large donations for the foundation. To fit in with wealthy donors, she believed that her children had to attend the best private schools and that she needed to travel and dress appropriately. She honestly believed that she was doing nothing wrong in taking "only a little" to meet these "needs."

It is critical that auditors understand how rationalizations of this kind underlie white collar crime. This executive director, an educated and upstanding citizen, fits the profile of most people they will encounter in an audit—yet there was a difference. Rationalization cuts right to the heart of the psychology of the fraudster: The ability of fraudsters to convince themselves that what they are doing is acceptable enables otherwise good people to do wrong things. Most people engage in rationalization daily, whether deciding to have a second portion of dessert, skip the last set of exercises, or play golf instead of mowing the lawn. But few people act as the executive director did, rationalizing fraud as ultimately in the best interest of the charitable foundation she served.

Looking back after the investigation had run its course, team members agreed that studying the executive director's actions and her deceits was the best training they had ever received about the value of professional skepticism (see Chapter 11).

KINDS OF RATIONALIZATION

In many admission-seeking interviews, suspects confess to their crimes, but rarely do they say, "I stole the money." Instead, they bring up their rationalization for the crime. Such rationalizations can be of many kinds:

- "It was a loan, and I had every intention of paying it back. See (*pulling out a spreadsheet*), I kept track of all my loans so that I could pay it all back one day."
- "That accounting rule is confusing and subjective. Accounting for the transactions in the manner I chose is entirely acceptable."
- "My boss has been cheating on his taxes for years. I'm just getting my share."
- "Everyone in this industry takes kickbacks. I'm sure my employer is aware of it, and that's why they don't pay me very much. They expect me to supplement my income with 'gifts' from our suppliers."
- "I'm the hardest working employee here, and I know my boss would give me a substantial raise if he could do it without other people knowing. Instead, I take a little bit, but I'm actually saving the company money because only I get the 'raise.' "
- "What do you expect me to do? You give me no health insurance coverage, and I need to provide for my children and my parents. They depend on me, and I can't let them down."
- "There are a lot of good people here. If I didn't make up a few entries to give the appearance to corporate that we were making budgeted income, they would close our division and put fifty people out of work. I did it to save their jobs."

In sum, rationalization enables a person to take that final step toward crime.

AUDITORS' NEED TO UNDERSTAND THE MIND OF THE FRAUDSTER

In the introduction to *Why Smart People Do Dumb Things,* Mortimer Feinberg and John J. Tarrant begin:

> *If you are of above average intelligence—and if you have mastered the use of high intelligence to solve problems and achieve goals—it is the premise of this book that you are at risk [of perpetrating a fraud] because of the strength of your cognitive equipment.*[15]

The book recounts tale after tale of successful professionals and politicians who did something dumb and ruined their lives. It is also a book that can help auditors understand the mind of the white collar criminal. Because auditors, within the time at their disposal, cannot verify every transaction, they must make assumptions based on

[15] Mortimer Feinberg and John J. Tarrant, *Why Smart People Do Dumb Things* (New York: Simon & Schuster, 1995), 11.

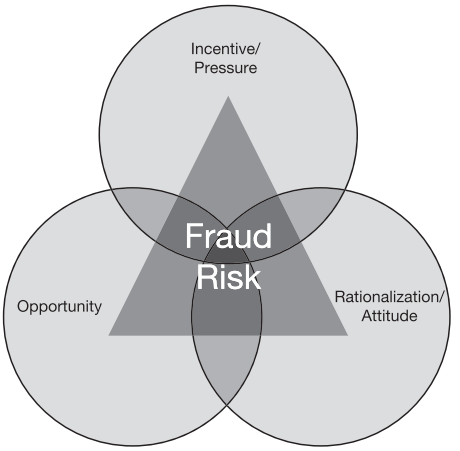


EXHIBIT 2.2 The Fraud Triangle

audit evidence gathered until the point of the decision. The more auditors understand about why criminals do what they do, the better prepared they may be to determine the nature, timing, and extent of audit procedures relative to the risks identified during the planning stage and modify these procedures, as may be warranted, on the basis of the audit evidence found. Professional skepticism is the attitude that must drive the financial statement audit. If we lived in a perfect world in which no one made mistakes, or lied, or cheated, or stole, audits would be unnecessary. But we don't, and so audits are required. Even with effective auditing, at the end of every audit and forensic accounting investigation, uncertainty will remain.

As auditors continue to focus on the fact that smart people do "dumb" things and on the conditions under which white collar criminals may act, auditors may be able to better select transactions worthy of expanded testing and know also how to evaluate the results of those tests. The so-called fraud triangle, shown in Exhibit 2.2, offers three conditions that tend to be present when frauds occur.

- Incentive or pressure
- Opportunity
- Rationalization and attitude

The fraud triangle is discussed in further detail in Chapter 13, but for now, it is sufficient to know that it takes all three conditions for a fraud to occur. The first two parts of the triangle, incentive and opportunity, are usually observable. The third condition, rationalization, is often the toughest of the three to identify. This is why auditors need to be ever vigilant to the possibility of fraud. A more informed understanding of the psychology of the fraudster usually makes for a better auditor.

CONCLUSION

As auditors focus on the number of people they encounter in the course of an audit, they would probably agree that a great many of those people would no doubt have

opportunities to commit fraud. How many others also have the undisclosed incentive and ability to rationalize their behavior, however, is harder to determine.

In the design of controls to prevent financial crime and in the performance of audit procedures, it is important to keep in mind the expression, "Locks on doors keep out honest people." Predators, as noted earlier, have a good chance of circumventing most of the controls a company puts in place. Fraud deterrence and detection controls are designed, theoretically, to stop everyone else, but they won't, because it is unrealistic to expect controls that can be designed to stop everyone. Collusion, for example, may defeat a well-designed control and may not be detected in a timely manner by individuals performing daily control activities.

The best fraud deterrence mechanism is simple: Create the expectation in your organization that wrongdoers will be caught and that punishment will be swift and commensurate with the offense. The emphasis on expectation is important. It can be brought about in a number of ways. Effective training and education on the importance of ethical conduct, background checks on all employees, regular fraud audits by forensic accounting investigators, and a strong internal control system are among the means. To create that perception, employees must also be well aware that their activities are being monitored, and all employees with access to financial assets and transactions must have a healthy respect for the robustness of the control system. If employees believe they will be caught and punished for wrongdoing, that belief may be enough to keep them from adding rationalization to incentive and opportunity.

Some experts have suggested that attention to the institutional level rather than the individual level can be fruitful. For example, Susan P. Shapiro wrote in *American Sociological Review,* "I suggest we begin sampling from settings of trust—legislatures, pension funds, hospitals, labor unions, probate or surrogates' courts, charities, law enforcement agencies, wire services, purchasing departments, universities—and examine how these fiduciaries define and enforce trust norms, the structural opportunities for abuse, the patterns of misconduct that ensue, and the social control pressures that respond."[16] This would provide greater understanding, she says, of the conditions that allow the individual to rationalize.

Be that as it may, auditors—working as necessary with forensic accounting investigators—realize that there could be a fraudster somewhere in the organization they're auditing. The fraudster may be a predator—an individual who works there to steal—or may be a seemingly upstanding citizen with a secret incentive such as a problem at home, a golden opportunity such as knowledge of a weakness in the control system, and a rationalization such as, "It doesn't really harm anyone." Of course, there is another possibility: outright greed.

[16] Susan P. Shapiro, "Collaring the Crime, Not the Criminal: Reconsidering the Concept of White-Collar Crime," *American Sociological Review* 55 (1990): 346–365.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 3

The Roles of the Auditor and the Forensic Accounting Investigator

James S. Gerson, John P. Brolly, and Steven L. Skalak

To understand the forensic accounting investigator's role in deterring, detecting, and investigating fraud—as distinct from the independent auditor's role as a financial statement examiner—we need to first recall the differences between what auditors do and what forensic accounting investigators do and why. Also, their professional worlds have changed in recent years, in ways that bear close examination.

The auditor's concern is that the financial statements of an entity be stated fairly in all material respects. Accordingly, the auditor's responsibility is to design and implement audit procedures of sufficient scope and depth to detect material deficiencies in the financial statements—essentially, without regard to the source or origin of the deficiency. Auditors are charged with making appropriate, reasonable efforts to detect material misstatements in financial statements and causing management to correct material misstatements or misrepresentations before the financial statements are shared with the user community or, alternatively, alerting investors not to place reliance on the statements through qualification of their professional opinion issued as part of the company's public filings. Even this seemingly simple statement of the auditor's mission brings into play a series of interrelated and complex concepts, including:

- Reasonable assurance
- Material misstatement
- Detection, as distinct from deterrence and investigation
- Expectations about the efficacy of the auditing process

The forensic accounting investigator has a largely separate set of concerns based on a different role that calls for different tools, different thought processes, and different attitudes. The forensic accounting investigator's concern is not with reaching a general opinion on financial statements taken as a whole, derived from reasonable efforts within a reasonable materiality boundary. Instead, the forensic accounting investigator's concern is, at a much more granular level, with the detailed development of factual information—derived from both documentary evidence and testimonial evidence—about the *who*, *what*, *when*, *where*, *how*, and *why* of a suspected or known impropriety. Sampling and materiality concepts are generally not used in

determining the scope of forensic accounting procedures. Instead, all relevant evidence is sought and examined. Based on the investigative findings, the forensic accounting investigator assesses and measures losses or other forms of damage to the organization and recommends and implements corrective actions, often including changes in accounting processes and policies or personnel actions or both. The forensic accounting investigator also takes preventive actions to eliminate recurrence of the problem. The forensic accounting investigator's findings and recommendations may form the basis of testimony in litigation proceedings or criminal actions against the perpetrators. They may also be used in testimony to government agencies such as the Securities and Exchange Commission in the United States or the Serious Fraud Office in the United Kingdom. Accordingly, the scope of the investigation and the evidence gathered and documented must be capable of withstanding challenges that may be brought by adversely affected parties or skeptical regulators.

Clearly, there are many commonalities between auditing and forensic accounting. Both rely on:

- Knowledge of the industry and the company, including its business practices and processes
- Knowledge of the generally accepted accounting principles of the jurisdiction in question
- Interpretation of business documents and records
- Independence and objectivity—perhaps the most important commonality

Another commonality is that both the auditor and the forensic accounting investigator must function effectively in the complex and ever-changing business environment. However, despite many common bases, audits are not the same as forensic accounting investigations. Two simple analogies will help convey the differences.

THE PATROLMAN AND THE DETECTIVE

Neither auditors nor forensic accounting investigators are law enforcement officers; while imperfect, however, a simplified analogy to patrolmen and detectives can help illustrate the auditor's challenge to detect material misstatements in financial statements in contrast to the forensic accounting investigator's mission to fully investigate allegations of a suspected impropriety.

A patrolman, working a particular shift, circulates through the community inspecting and observing its visible elements for signs of improper behavior ranging from minor infractions of municipal ordinances to evidence that a major crime may have been committed. The patrolman selects his route based on past experience, the time of day, and the length of his shift, and adjusts it for any particular observations during his patrol. He knows these judgments and adjustments to the patrol are necessary because no matter how much he might like to be continuously present at every location in the community, it is impossible to do so. So, too, with the auditor, who examines a selected sample of transactions to support the opinion on the financial statements and, based on those results, decides whether to examine more, whether to change the audit technique or test, or whether to conclude on the basis of procedures already completed. These decisions are based in large part on her assessment of the

risk of material misstatement based on both past experience and current evidence. Auditors might like to go everywhere in a company and examine every transaction but, because, like the patrolman, they cannot be everywhere at all times, they must determine when and where to concentrate their procedures.

The analogy of detective work is similarly instructive of the forensic accounting investigator's mission. As compared to patrol officers, who circulate throughout the community concentrating on high-risk areas, detectives are not on patrol. They are called in once a crime is suspected or observed. These related but differing activities—routine patrolling and criminal investigation—can be balanced with relative ease. If greater deterrence is needed, more patrol officers covering more territory more often is a solution. Similarly, if there are many crimes or if there is a highly complex situation to investigate, then assigning more detectives, or in the financial context, more forensic accounting investigators, is a solution.

While it is clear that forensic accounting and detective work are roughly analogous, the analogies between issues confronting the auditor and the patrol officer—namely, how detailed should observations be in varying circumstances—are less obvious. Take the example of a garage—the customary storage location for a reasonably valuable asset: a car. A patrol officer who drives by in the middle of the night might observe any of the following circumstances:

- Garage door closed, light off
- Garage door closed, light on
- Garage door open, light off
- Garage door open, light on, car visible
- Garage door open, light on, no car

In each case, the officer has choices, informed by knowledge of the community, past experience on patrol, knowledge of the home owner, if any, and overall security conditions in the community. If the door is closed, the light is off, and the officer drives by without stopping, few would argue neglect of duty. If the door is closed and the light on, the likely explanation is that the owner just got home and the garage door light has not gone out yet or was left on by accident. If the officer comes into the yard, looks in the garage window, sees the car and no other activity, and then leaves, almost everyone would agree that the officer has performed a careful, thorough patrol. Even if the officer drives by without looking more closely—on the assumption that the light was left on by accident—few would conclude that the officer was remiss in his duty. And even if a crime were silently in progress in a back room of the house, no one would fault the officer for failing to detect it from the visible evidence.

Conversely, if you were that home owner and the officer rang your doorbell, woke you from a sound sleep, told you your car was safe and sound in the garage but the garage light needed to be turned off, you'd almost certainly consider the officer overly zealous and inconsiderate, even if you agreed in principle that the light should not burn through the night.

Contrast this scenario with another. The officer spots the garage light on and the door open, comes up your driveway for a better look, sees that everything is in order, and leaves. An hour later, someone steals the entire contents of your garage. If you were to find out that the officer had been on the scene an hour beforehand and

did not wake you to suggest closing the garage door, you might well be disappointed with the officer's judgment, although, truth be told, you would have been annoyed had the officer awakened you and urged you to close the door and turn off the light. Complaining loudly about the inconvenience and offering the helpful thought that there must be better things for police officers to do with their time, you would nonetheless have risen, turned off the light, and closed the door.

We all can imagine a wide range of scenarios related to patrol officers and their choices, and there will be a spectrum of views about how much investigation is appropriate. Some risk-averse residents would no doubt prefer that the officer check on whether their car is still there, even if the light is off and the door closed. Others would take the view that checking is too costly for the minimal risk evident in that circumstance. And still others would assert a right to privacy, perhaps saying that even if the light is on and the door open, stay away unless a crime is obviously in progress.

Like the patrol officer, the auditor sits outside the client company, looking in at its operations with a less-than-complete view of everything that is going on. Like the patrol officer, the auditor cannot be in all places in the company at once, cannot visit every location in each period, and can sample transactions only at visited locations rather than examining every transaction. Furthermore, before going out on an audit, the auditor must select the timing, location, and nature of the transactions or controls to be examined—that is, make judgments about the scope of the audit work. Finally, in examining the items sampled—like the patrol officer observing the garage—the auditor has to balance risk and expectations to decide the correct scope of any further examination. An auditor who finds a potential issue must decide whether to expand the audit, for example, by further inquiry, or decide to conclude on the basis of the available evidence that nothing improper is indicated. Choices and judgments, large and small, abound throughout the audit process.

In contrast, the forensic accounting investigators can be compared to the detectives called in to investigate a crime, like the theft of the car. The detectives will examine the scene of the crime, question everyone who might be able to shed light on the theft, and bring to bear a host of specialized forensic resources to gather any and all clues that might exist. This is a specialized, time-consuming, and costly mission not directly connected with the original mission of patrolling the community to ascertain that everything is substantially in order. After all of their effort, the detectives may find out only that your child—a newly licensed teenage driver—decided to take the car down by the river to practice guitar without disturbing you. On the other hand, they may uncover a car theft ring. It might make sense to call upon the detectives more frequently, but consideration must be given to the ratio of detectives to patrol officers (there just are not as many) and to the cost of detectives, which is typically higher than that of patrol officers. Judgments are made that balance the community's desire for safety with the cost it is willing to pay for such comfort.

The fundamental challenge is to integrate the greater depth of investigation by the forensic accounting investigator into the audit when it is appropriate to do so—either by calling in forensic accounting investigators to investigate or by adapting some of their own procedures to an appropriate extent so they can continue to meet the requirements of the profession, the client, and the public and to restore or enhance confidence in the accuracy of the conclusions of an audit. The problems, judgments, and expectations illustrated in this analogy permeate the environment in which

auditors conduct audits and forensic accounting investigators conduct investigations. But that environment is characterized by a greater degree of complexity than can be illustrated through simple analogies. These complexities and their impact should be neither overlooked nor underestimated.

COMPLEXITY AND CHANGE

The worlds of the auditor and the forensic accounting investigator are complex, fast paced, constantly changing, and diverse. Complexity and change are important considerations for both because, separately and together, they create uncertainty about the outcome of business affairs. The quest for certainty in business affairs motivates businesses and businesspeople the world over to take charge, exercise control, hedge risks, and secure the bottom line (see Exhibit 3.1). In some cases, this basic desire for control will give rise to improper activities in the conduct of business—for example, unfair competitive practices, false advertising, price fixing, breach of contract, and circumvention of regulations. In other cases, in which control is desired but cannot be obtained or when efforts are unsuccessful or not yet successful, false reports of success may be issued (see Chapter 21). While complexity and change are not in and of themselves negative, business failures have time and time again shown that the combination of the two creates uncertainties that may motivate improper business behavior on the part of employees and executives. Auditors and forensic accounting investigators must appreciate this dynamic to carry out their respective roles effectively.

Today's business world is complex. Global competition, instantaneous global communications, advances in science and technology, risks unknown even 10 years ago, and many other factors define today's business life. We are working harder and

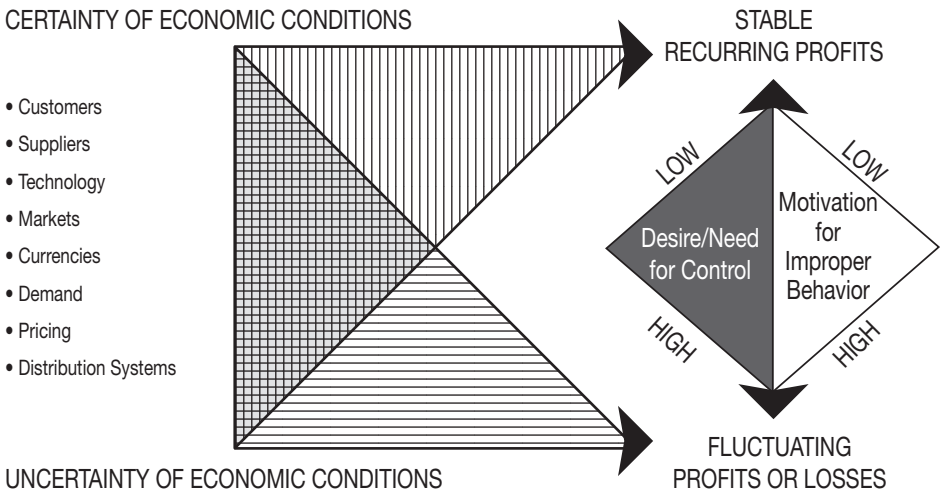


EXHIBIT 3.1 Types of Pressure on Executives

longer and dealing with high levels of rapid and frequent change that few could have expected or predicted.

Open that most basic of corporate communications—the annual report—and it will be evident how much has changed. Companies are offering an astounding number and diversity of products and services. Old models that distinguished one industry from another have blurred, as industrial companies can look in some respects like banks, while banks can look like investment banks, security dealers, and insurers. Management's discussion and analysis in virtually any annual report will probably reveal many different complexities and changes confronting the business, some of which are inventoried in Exhibit 3.2.

Among the factors in Exhibit 3.2, some are more critical than others:

- *Ever-increasing globalization adds greatly to the complexity of today's business world.* Controlling diverse organizations around the world and ensuring that they understand and meet the company's business objectives while operating ethically require a thorough understanding of local economic and political conditions as well as customs, laws, and regulations at each key location.
- *Information technology, while adding enormously to business productivity, has intrinsic challenges.* As companies exchange information internally and with their suppliers and customers on a real-time basis through the Internet and struggle to keep up with technological advances, the challenge to keep corporate information relevant, reliable, secure, and private is very real. Outsourcing is becoming more and more common as companies recognize the complexity and cost of meeting these requirements.

Very important to companies and their auditors is the complexity of today's financial reporting rules and regulations. To operate effectively in an increasingly complex world, companies and their auditors must be capable of continuous learning, interpretation, and application of complex and ever-changing rules.

- *And as if these complexities were not enough, the pace of change continues to accelerate, challenging companies as never before to keep up.* In the past few years, trillions of dollars in new wealth among millions of investors have evaporated—in many cases, just as quickly as that wealth had accumulated. Success is often fleeting, and failure to meet expectations rarely escapes punishment by the capital markets.

AUDITOR ROLES IN PERSPECTIVE

While both management and the auditor address some of the same issues, their roles are vastly different. There has been some confusion on this point, especially within the general public, which tends to attribute to the auditor certain responsibilities that actually rest with management. The professional standards of the American Institute of Certified Public Accountants (AICPA) have long made clear that the financial statements and the decisions shaping the financials are the responsibility of management.

EXHIBIT 3.2 Twenty-First-Century Business Complexity

Business Structure

- More than one industry within the company—for example, automotive manufacture and financial services under one roof
- Global scope of customers, vendors, and operations
- Interdependence between the company and its suppliers, customers, and competitors through:
  - Outsourcing arrangements
  - Joint ventures
  - R&D contracts
  - Marketing agreements
  - Cross-ownership and board membership
  - Shared facilities
  - Industry standardization of technical or documentary requirements
- No two companies exactly alike

Business Methods

- Information technology that's automating business processes from the factory floor to headquarters
- Instantaneous global communications
- Internet-enabled business systems for dealing with external parties
- Paperless business processes updated in real time
- Complex financial, insurance, and hedging arrangements to control risks

Rules and Regulations

- Voluminous rules governing all aspects of business life
- Complex accounting and reporting requirements in separate jurisdictions worldwide
- Complex judgments requiring a mix of information about the past, present, and future
- Aggressive enforcement and low public tolerance for error or failure

Social Trends

- Increased employee mobility and decreased loyalty
- Reduced security over data and intellectual property
- Demands for short-term success
- Economic disparity among countries or markets or both
- Economic disparity among people within countries or markets or both
- Increasing indebtedness of Western nations and increasing wealth accumulation by emerging economies
- Cultural diversity within the business world
- Differences in transparency and objectivity of press or other reports about a particular location or subject
- Public health crises, food and water shortages, HIV/AIDS, severe acute respiratory syndrome
- Speed of medical and technological changes
- Political change such as events in the Middle East and periodic turmoil in South America
- The threat and reality of terrorist attacks and efforts geared toward extensive homeland security

The financial statements are management's responsibility. The auditor's responsibility is to express an opinion on the financial statements. Management is responsible for adopting sound accounting policies and for establishing and maintaining internal control that will, among other things, record, process, summarize, and report transactions (as well as events and conditions) consistent with management's assertions embodied in the financial statements. The entity's transactions and the related assets, liabilities, and equity are within the direct knowledge and control of management. The auditor's knowledge of these matters and internal control is limited to that acquired through the audit. Thus, the fair presentation of financial statements in conformity with generally accepted accounting principles is an implicit and integral part of management's responsibility.[1]

Enlarging on these concepts in a much-cited court opinion, the judge in *Bily v. Arthur Young*[2] memorably stated:

> *An auditor is a watchdog, not a bloodhound. . . . As a matter of commercial reality, audits are performed in a client-controlled environment. The client typically prepares its own financial statements; it has direct control over and assumes primary responsibility for their contents. . . . The client engages the auditor, pays for the audit, and communicates with audit personnel throughout the engagement. Because the auditor cannot in the time available become an expert in the client's business and record-keeping systems, the client necessarily furnishes the information base for the audit. Thus, regardless of the efforts of the auditor, the client retains effective primary control of the financial reporting process.*[3]

NOT ALL GOOD PEOPLE

The overwhelming majority of corporate managements do the right thing when it comes to financial reporting.[4] Still, there are some who do not. Complicating matters is the fact, according to the SEC, that the majority of large and complex corporate frauds are perpetrated by top management—the very people charged with responsibility for the quality of the company's financial reporting. A recent SEC staff report confirmed this observation. A review of the commission's major enforcement cases in 2009, including subprime-related securities, auction rate securities, Ponzi schemes, mutual funds, broker-dealers, financial fraud, issuer disclosure, and insider

[1] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 1 (§ 110), *Codification of Auditing Standards and Procedures,* revised, April 1989, to reflect conforming changes necessary due to the issuance of SAS 53 through 62. As amended, effective for audits of financial statements for periods beginning on or after January 1, 1997, by SAS 78. Paragraph renumbered by the issuance of SAS 82, February 1997. Revised, April 2002, to reflect conforming changes necessary due to the issuance of SAS 94. (Codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 110, par. 3.)
[2] *Bily v. Arthur Young and Co.*, 3 Cal. 4th 370, 11 Cal. Rptr. 2d 51, 834 P.2d 745 (1992).
[3] Id.
[4] PricewaterhouseCoopers, *PricewaterhouseCoopers LLP 2002 Securities Litigation Study,* 7, http://10b5.pwc.com/PDF/2002_STUDY_FINAL.PDF.

trading showed that most cases involved charges against at least one senior manager.[5] As the Public Oversight Board (predecessor of today's Public Company Accounting Oversight Board [PCAOB]) pointed out:

> *On the one hand, to accomplish the audit requires the cooperation of management; on the other hand, management is in a position to mislead the auditors in their quest for valid evidence.*[6]

EACH COMPANY IS UNIQUE

Auditors and forensic accounting investigators know that each company is unique and that they must understand and respond to those unique characteristics if they are to be effective. While the list is virtually endless, the ways in which companies can be highly distinct from one another include corporate governance; ownership and organizational structure; industry; products and services; size and geographic reach; business objectives and risks; key business processes and systems; relationships with customers, suppliers, and other business partners; management style and attitudes; management experience and competence; internal control; and accounting policies.

ROLE OF COMPANY CULTURE

A company's culture consists of its shared history, values, beliefs, and goals. To this must be added the shared operating style—at all levels and in all parts of the organization—through which behavior in keeping with the culture is encouraged and rewarded, while conduct that disregards or defies the culture is deterred, detected, and eliminated or, if need be, penalized.

Appearances can deceive. The need to discern the substance of a company's culture and not be swayed by form or appearance is key for both forensic accounting investigators and auditors. Codes of conduct, ethics statements, and conflict-of-interest policies are important, but unfortunately, some companies have all those documents in place yet fall far short of honoring them. Essential to fostering a healthy and widely shared corporate culture are the commitment and attitudes of top management, vigilantly monitored by an engaged board of directors. The lofty phrase *tone at the top* is often heard in discussions of these matters, but a rough proverb is more to the point: "A fish rots from the head."

The CPA's Handbook of Fraud and Commercial Crime Prevention[7] compares the environment and culture of entities with a high potential for fraud with entities that are far less likely to experience or generate fraud.

---

[5] U.S. Securities and Exchange Commission, *2009 Performance and Accountability Report,* www.sec.gov/about/secpar/secpar2009.pdf.

[6] Public Oversight Board, Panel on Audit Effectiveness, *Report and Recommendations* (2000), Chap. 3, § 3.45, 86, www.pobauditpanel.org/downloads/chapter3.pdf.

[7] T. Avey, T. Baskerville, and A. Brill, *The CPA's Handbook of Fraud and Commercial Crime Prevention* (New York: American Institute of Certified Public Accountants, 2002).

The factors listed in Exhibit 3.3 are only representative or directional indicators of what may likely be encountered within a business and should be supplemented by the knowledge of the individuals experienced on the engagement. There will frequently be exceptions to these general characteristics; there is no substitute for good judgment. In one matter, a senior executive of a subsidiary would annually participate in the planning process and include in the budget the amount of money he intended to steal. In this way, his expenses never exceeded the plan. He escaped detection for more than ten years.

ESTIMATES

Another area that often causes complexity in financial reporting, as well as confusion among users, is the pervasive need for estimates. Estimates appear in financial statements because of the continuous nature of business. Unlike a footrace that ends at the finish line or an athletic contest that ends with the final buzzer, a business and its transactions are continually in varying stages of completion. There are many items in a financial statement for which the final outcome is not known with precision.

Given the complexity and continuity of business, it is difficult to capture a clear snapshot of a company's financial position and performance at a particular point in time. As a general matter, estimates are most commonly made concerning the final amounts of cash that will be received or paid once assets or liabilities are finally converted into cash. Such estimates can encompass, for example, allowances for uncollectible customer receivables, estimates of liabilities for claims or lawsuits brought against a company, the amount of profit or loss on a long-term contract, and the salability of inventory that is past its prime. Most estimates are based on three types of information: past performance of the same or similar items, what is currently occurring, and what management believes will be the probable outcome. Further complicating matters, the weight to assign each type of information varies depending on the particular circumstances. But no matter how determined, unlike the score of a sporting contest, an estimate in financial statements is a prediction of what will happen, not the objective tally of what has already taken place.

In the financial and credit crisis of 2008 and 2009, estimates of asset values used by banks and other capital market participants for illiquid securitizations of mortgage-backed securities were widely criticized. Some commentators went so far as to suggest that the accounting requirement to estimate fair value of these securities and record the changes in that value as an item of profit and loss were a contributing cause of the crisis, as opposed to a mere reporting of the problem. Whichever side of the argument one favors, the circumstances of the recent crisis serve to illustrate the pervasive and significant impact of estimation processes on public financial reports and their importance to the functioning of the market as a whole.

Estimates can create difficult challenges for auditors. The following Public Oversight Board report addresses the significance of estimates and their implications to auditors.

> *. . . the amounts involve subjective estimation and judgment. Unlike most third-party transactions, the amounts involved are not fixed. They may be based on a range of potential results, and reasonable people may disagree on the most likely outcome or amount.*

EXHIBIT 3.3 Environmental and Cultural Comparison of Those Organizations with High Fraud Potential and Those with Low Fraud Potential

Variable	High Fraud Potential	Low Fraud Potential
1. Management style	a. Autocratic	a. Participative
2. Management orientation	a. Low trust b. Power driven	a. High trust b. Achievement driven
3. Distribution of authority	a. Centralized, reserved by top management	a. Decentralized, dispersed to all levels, delegated
4. Planning	a. Centralized b. Short range	a. Decentralized b. Long range
5. Performance	a. Measured quantitatively and on a short-term basis	a. Measured both quantitatively and qualitatively and on a long-term basis
6. Business focus	a. Profit focused	a. Customer focused
7. Management strategy	a. Management by crisis	a. Management by objective
8. Reporting	a. Reporting by routine	a. Reporting by exception
9. Policies and rules	a. Rigid and inflexible, strongly policed	a. Reasonable, enforced fairly
10. Primary management concern	a. Capital assets	a. Human, then capital and technological assets
11. Reward system	a. Punitive b. Penurious c. Politically administered	a. Generous b. Reinforcing c. Administered fairly
12. Feedback on performance	a. Critical b. Negative	a. Positive b. Stroking
13. Interaction mode	a. Issues and personal differences skirted or repressed	a. Issues and personal differences confronted and addressed openly
14. Payoffs for good behavior	a. Mainly monetary	a. Recognition, promotion, added responsibility, choice assignments, plus money
15. Business ethics	a. Ambivalent, rides the tide	a. Clearly defined and regularly followed
16. Internal relationships	a. Highly competitive, hostile	a. Friendly, competitive, supportive
17. Values and beliefs	a. Economic, political, self-centered	a. Social, spiritual, group centered
18. Success formula	a. Works harder	a. Works smarter
19. Human resources	a. Burnout b. High turnover c. Grievances	a. Not enough promotional opportunities for all the talent b. Low turnover c. Job satisfaction
20. Company loyalty	a. Low	a. High

EXHIBIT 3.3 (*Continued*)

Variable	High Fraud Potential	Low Fraud Potential
21. Major financial concern	a. Cash flow shortage	a. Opportunities for new investments
22. Growth pattern	a. Sporadic	a. Consistent
23. Relationship with competitors	a. Hostile	a. Professional
24. Innovativeness	a. Copycat, reactive	a. Leader, proactive
25. CEO characteristics	a. Swinger, braggart, self-interested, driver, insensitive to people, feared, insecure, gambler, impulsive, tightfisted, numbers and things oriented, profit seeker, vain, bombastic, highly emotional, partial, pretends to be more than she is	a. Professional, decisive, fast paced, respected by peers, secure risk taker, thoughtful, generous with personal time and money, people, products, and market oriented, builder, helper, self-confident, composed, calm, deliberate, even disposition, fair, knows who she is, knows what she is, and knows where she is going
26. Management structure, systems and controls	a. Bureaucratic b. Regimented c. Inflexible d. Imposed controls e. Many-tiered structure, vertical f. Everything documented, a rule for everything	a. Collegial b. Systematic c. Open to change d. Self-controlled e. Flat structure, horizontal f. Documentation adequate but not burdensome, some discretion afforded
27. Internal communication	a. Formal, written, stiff, pompous, ambiguous	a. Informal, oral, clear, friendly, open, candid
28. Peer relationships	a. Hostile, aggressive, rivalrous	a. Cooperative, friendly, trusting

Source: The CPA's Handbook of Fraud and Commercial Crime Prevention (2000, 2001), by the American Institute of Certified Public Accountants.

> *. . . activity in reserves may be driven principally by management's intentions and decisions rather than by external events or transactions. (For example, management has the ability to determine whether it will offer to settle outstanding litigation.) Indeed, determining just when management's intentions create a liability has vexed accountants and auditors for decades, and, for example, has been a significant factor in the uncertainties surrounding the accounting for restructuring and similar reserves.*[8]

[8] Public Oversight Board, Panel on Audit Effectiveness, *Report and Recommendations* (2000), Chap. 2, §§ 2.148–2.150, 50, www.pobauditpanel.org/downloads/chapter2.pdf.

All of these features could have an impact on a forensic accounting investigation into the propriety of an estimate that turns out to be incorrect. A legitimate assertion of managerial confidence in the business's ability to achieve certain estimated results is one thing. A deceptive misinterpretation that is intended to generate a favorable estimate is another thing altogether and may pose a substantial investigative challenge. The forensic accounting investigator is often vexed by the myriad complexities and alternative rationales that may be offered to explain the difference between an estimate and an actual result. Given that estimates often constitute the cause of material differences in financial statement presentations, the ability to distinguish between the manipulatively self-serving and the merely incorrect is a critical element of many investigations.

CHOICES

In addition to judgments about estimates, there are many other areas in which management uses judgment and makes choices that affect the company's reported financial results. Obviously, management is paid to make judgments and develop strategies that affect the results of the business over time—in both the short and long terms. The challenge for accountants is to reflect objectively and properly the impact of those decisions—without regard to the underlying motivation. However, when the motivation for a transaction is solely to obtain the accounting impact of its recognition, then the business merits of the transaction may be questionable. While some of these so-called earnings management decisions must be recorded because they have in fact taken place, others often have features or terms that require careful evaluation of their legitimacy. Complicating this is that there is often no bright line differentiating the acceptable from the unacceptable, so that management and the auditor may spend a great deal of time focusing on the large expanse of gray areas in which management's decisions can significantly affect reported earnings.

Some earnings management activities involve legitimate discretionary choices of when to enter into transactions that require accounting recognition, not unlike legitimate year-end tax-planning decisions made to accelerate deductions or defer taxable income. For example, advertising expenditures, which generally should be expensed when incurred, may be accelerated in the fourth quarter if the entity is exceeding its earnings target or deferred if it is failing to meet that target. This would generally be an appropriate earnings management technique. Other earnings management activities involve legitimate choices of how to account for transactions and other events and circumstances—particularly those involving accounting estimates and judgments—in conformity with Generally Accepted Accounting Principles (GAAP). For example, implementation of a decision to enhance the entity's credit and collection activities may legitimately support reducing the estimate of bad debt expense.[9]

Unfortunately, as the Public Oversight Board has pointed out, earnings management may also involve intentionally recognizing or measuring transactions and other events and circumstances in the wrong accounting period or recording fictitious

[9] Id., Chap. 3, § 3.15, 78, www.pobauditpanel.org/downloads/chapter3.pdf.

transactions, both of which constitute fraud. The Public Oversight Board provides the following example of the potential for improper earnings management in one of the most difficult areas: revenue recognition.

Assume that an entity announces that—either in response to higher costs, to meet current-period sales targets, or for any other reason—it will increase prices at the beginning of the next quarter, thereby stimulating some customers to purchase unusually high quantities before the end of the current quarter. If the sales meet all the criteria for revenue recognition, the entity should recognize the sales when the product is shipped, possibly resulting in an effective and legitimate management of earnings. If, however, there is an unusual right-of-return privilege and there is no basis for estimating the returns that will take place, the transaction essentially becomes a conditional sale, and recognizing the revenue when the product is shipped violates GAAP and misstates the financial statements. If the right-of-return privilege has been concealed from the auditor as part of a scheme to increase reported earnings, the financial statement misstatement involves fraudulent financial reporting.[10]

WHAT AUDITORS DO

Why is it unrealistic to assume that all material financial statement frauds can be detected? This can be answered by the Statement on Auditing Standards (SAS) No. 1, which sets out the auditor's fundamental responsibility:

> *The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. This Statement establishes standards and provides guidance to auditors in fulfilling that responsibility, as it relates to fraud, in an audit of financial statements conducted in accordance with generally accepted auditing standards.*[11]

To further understand this answer, three fundamental concepts must be examined. They are the difference between error and fraud as it relates to the auditor's responsibility, the meaning of *reasonable assurance*, and materiality.

Fraud versus Error

U.S. auditing standards state that the main difference between fraud and error is intent. Errors are *unintentional* misstatements or omissions of amounts or disclosures in financial statements.[12] Errors may involve:

[10] Id., Chap. 3, § 3.16, 78.
[11] American Institute of Certified Public Accountants, *Statement on Auditing Standards* (SAS) No. 1 (§ 110), 78, and 82, paragraph added, effective for audits of financial statements for periods ending on or after December 15, 2002, by SAS 99 (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 110, par. 2).
[12] American Institute of Certified Public Accountants, AICPA Professional Standards—U.S. Auditing Standards—AU § 312, *Audit Risk and Materiality in Conducting an Audit,* par. 7.

- Mistakes in gathering or processing data from which financial statements are prepared
- Unreasonable accounting estimates arising from oversight or misinterpretation of facts
- Mistakes in the application of accounting principles related to amount, classification, manner of presentation, or disclosure[13]

Fraud, on the other hand, is defined in SAS 99 as an *intentional* act that results in a material misstatement.[14] The motive or intent of an individual in making accounting entries is not the primary focus of the auditor's procedures. Auditors direct their efforts toward determining objectively measurable criteria regarding account balances and transactions by asking: Do the assets exist? How much was paid? What is the basis of the estimate? Is it reasonable? How much was collected? Were the goods shipped to the customer? By asking questions such as these and obtaining evidence to support the estimate where appropriate, auditors can be better positioned to ascertain that the amounts in the books are correct. If by all of these criteria, transactions have been recorded and reflected correctly in the financial results, then the intent of management in initiating and completing the transactions is irrelevant to the auditor. It is reasonable to presume that the transactions have been undertaken for appropriate corporate purposes, generally making profits in the current period or preparing to do so in the future. Thus, given the focus of the auditor, intent is not uniformly relevant; evaluation of intent is a subjective as opposed to an objective evaluation, and ascertaining intent is a difficult exercise. SAS 99 comments directly on the question of intent:

> *Intent is often difficult to determine, particularly in matters involving accounting estimates and the application of accounting principles. For example, unreasonable accounting estimates may be unintentional or may be the result of an intentional attempt to misstate the financial statements. Although an audit is not designed to determine intent, the auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether the misstatement is intentional or not.*[15]

Reasonable Assurance

Why is it that auditors cannot provide better than reasonable assurance? Why not provide absolute assurance?

---

[13] Id., par. 6.

[14] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par. 5.

[15] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit* (superseded by SAS 99 and codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), fn 3.

Professional auditing standards explain that the auditor cannot guarantee that the financial statements are entirely free of material misstatement and cannot provide absolute assurance for two reasons: the nature of audit evidence and the characteristics of fraud. The first reason audits cannot provide absolute assurance—the nature of audit evidence—springs in part from the practice that auditors test only selectively the data being audited. They do not audit all subsidiaries and divisions, all accounts, or all transactions. There are not enough auditors in the world to audit everything, and even if there were, a company's operations would grind to a halt, timely audited financial statements would be an impossibility, and the cost of an audit in strictly financial terms—that is, the auditor's fee—would be prohibitive. Auditors, by necessity, make judgments about the areas to be audited and the nature, timing, and extent of the tests to be performed. Also, auditors use their judgment in interpreting the results of their work and in evaluating audit evidence, especially with regard to areas dependent on management's judgments, such as significant accounting estimates. As a result of these factors, the auditor often has to rely on evidence that is persuasive rather than conclusive. This distinction is important when it comes to the subjective areas of an audit such as estimates, and as discussed later, in certain situations in which a fraud is being concealed. The distinction is explicitly cited in auditing standards concerning audit evidence.[16]

The second reason audits cannot provide absolute assurance involves the characteristics of fraud, particularly fraud based on collusion among management or falsified documentation, including forgery that serves to inhibit or prevent the auditor from detecting the related misstatements. Fraud, by nature, is hidden. It is buried in financial statement accounts and hidden in transactions in subledgers and account

[16] American Institute of Certified Public Accountants, AICPA Professional Standards—U.S. Auditing Standards—AU § 326, *Evidential Matter*, par. 22 and 23. These paragraphs explain that the auditor must typically rely on evidence that is persuasive as opposed to convincing because of the time and cost parameters under which an audit necessarily takes place to retain its usefulness. Specifically: "(22) The independent auditor's objective is to obtain sufficient competent evidential matter to provide him or her with a reasonable basis for forming an opinion. The amount and kinds of evidential matter required to support an informed opinion are matters for the auditor to determine in the exercise of his or her professional judgment after a careful study of the circumstances in the particular case. However, in the great majority of cases, the auditor has to rely on evidence that is persuasive rather than convincing. Both the individual assertions in financial statements, and the overall proposition that the financial statements as a whole are fairly presented, are of such a nature that even an experienced auditor is seldom convinced beyond all doubt with respect to all aspects of the statements being audited. [Paragraph renumbered by the issuance of Statement on Auditing Standards No. 48, July 1984. Paragraph subsequently renumbered and amended, effective for engagements beginning on or after January 1, 1997, by the issuance of Statement on Auditing Standards No. 80.](23) An auditor typically works within economic limits; the auditor's opinion, to be economically useful, must be formed within a reasonable length of time and at reasonable cost. The auditor must decide, again exercising professional judgment, whether the evidential matter available to him or her within the limits of time and cost is sufficient to justify expression of an opinion. [Paragraph renumbered by the issuance of Statement on Auditing Standards No. 48, July 1984. Paragraph subsequently renumbered by the issuance of Statement on Auditing Standards No. 80, December 1996.]"

reconciliations. If buried in an account that rolls up with hundreds of others into one line item on the income statement, it then gets transferred to retained earnings and becomes hidden from sight in future periods. AU 230, *Due Professional Care in the Performance of Work,* states in this regard:

> *Because of the characteristics of fraud, a properly planned and performed audit may not detect a material misstatement. Characteristics of fraud include (a) concealment through collusion among management, employees, or third parties; (b) withheld, misrepresented, or falsified documentation; and (c) the ability of management to override or instruct others to override what otherwise appears to be effective controls. For example, auditing procedures may be ineffective for detecting an intentional misstatement that is concealed through collusion among personnel within the entity and third parties or among management or employees of the entity. Collusion may cause the auditor who has properly performed the audit to conclude that evidence provided is persuasive when it is, in fact, false. In addition, an audit conducted in accordance with generally accepted auditing standards rarely involves authentication of documentation; nor are auditors trained as or expected to be experts in such authentication. Furthermore, an auditor may not discover the existence of a modification of documentation through a side agreement that management or a third party has not disclosed. Finally, management has the ability to directly or indirectly manipulate accounting records and present fraudulent financial information by overriding controls in unpredictable ways.*[17]

Most people would agree that auditors cannot provide absolute assurance that material misstatements do not exist. This is so despite the best efforts of auditors and despite the desire and the unrealistic expectation on the part of the user and regulatory communities that auditors will provide that assurance. Because of the matters noted earlier, there exists a difference between what auditors actually do and what the public may expect them to do.

Materiality

The standard auditor's report includes the following expression or its equivalent: "In our opinion, the accompanying financial statements present fairly, *in all material respects* . . ." [emphasis added]. In other words, auditors are responsible for providing reasonable assurance that the financial statements are stated fairly—but only with regard to material matters.

---

[17] American Institute of Certified Public Accountants, AICPA Professional Standards—U.S. Auditing Standards—AU § 230, *Due Professional Care in the Performance of Work,* par. 12. [Paragraph added, effective for audits of financial statements for periods ending on or after December 15, 1997, by Statement on Auditing Standards No. 82. As amended, effective for audits of financial statements for periods beginning on or after December 15, 2002, by Statement on Auditing Standards (SAS) No. 99.]

The Financial Accounting Standards Board describes the concept of *materiality* as follows:

> *The omission or misstatement of an item in a financial report is material if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.*[18]

This formulation is in substance equivalent to the holding of the U.S. Supreme Court that a fact is material if there is "a substantial likelihood that the... fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[19] The concept of materiality recognizes that some matters, either individually or in the aggregate, are important to the fair presentation of financial statements in accordance with GAAP, while other matters are not important.

The SEC addresses the issue of materiality in Staff Accounting Bulletin (SAB) 99, *Materiality,* in the following terms:

> *The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.*[20]

Historically, many auditors may have focused on a standard of 5 percent of pretax income (loss) or after-tax income (loss) from continuing operations as the benchmark for materiality. However, based upon the nature and circumstances of the company being audited, other elements of the financial statements might be considered to be more appropriate measurements of what is of greatest significance to financial statement users. Such measures include operating earnings, gross profit, current assets, net working capital, total assets, total revenues, total equity, and cash flows from operations. Furthermore, SAB 99 cautions the auditor not to place exclusive emphasis on amounts, per se: "... misstatements are not immaterial simply because they fall beneath a numerical threshold."[21]

The guidance provided for auditors in SAS 99, *Consideration of Fraud in a Financial Statement Audit,* warns auditors that their procedures cannot be driven by materiality concerns alone, and they must take a view toward the nature of

---

[18] American Institute of Certified Public Accountants, Statement of Financial Accounting Concepts No. 2, *Qualitative Characteristics of Accounting Information,* par. 132.
[19] *Basic, Inc. v. Levinson,* 485 U.S. 224 (1988).
[20] U.S. Securities and Exchange Commission, SEC Staff Accounting Bulletin: No. 99—*Materiality,* 17 CFR Part 211 [Release No. SAB 99], www.sec.gov/interps/account/sab99.htm.
[21] Id.

the error and by whose hand it was committed.[22] Judgments about materiality are among the most difficult auditors are required to make. The auditor—as well as the company—considers materiality from both quantitative and qualitative standpoints. In quantitative terms, there are no hard-and-fast rules; the auditor looks at the impact of identified misstatements—both separately and in the aggregate—and considers whether in relation to individual amounts, subtotals, or totals in the financial statements, they materially misstate the financial statements taken as a whole. From a qualitative standpoint, misstatements of relatively small amounts that come to the auditor's attention could have a material effect on the financial statements. For example, an illegal payment of an immaterial amount could be material if there is a reasonable possibility that it could lead to a material contingent liability or a material loss of revenue.

BEDROCK OF AN EFFECTIVE AUDIT

The auditing profession and regulatory authorities—CPA firms, industry standard setters like the AICPA, and regulators including Congress, the SEC, and the Public Company Accounting Oversight Board (PCAOB)—are all working to maintain investor confidence in financial reporting. This is manifest in SAS 99 and in the requirements of the Sarbanes-Oxley Act and in the ongoing work of the PCAOB to revise auditing standards. Despite these changes, the bedrock of an effective and high-quality audit process still consists of competence and the professional attitude of individual auditors. These attributes consist primarily of professional skepticism, knowledge and experience, and independence and objectivity. These form the bedrock of an effective audit.

Professional Skepticism

SAS 99 summarizes the importance of professional skepticism in the auditor's approach to possible fraud:

> *Because of the characteristics of fraud, the auditor's exercise of professional skepticism is important when considering the risk of material misstatement due to fraud. Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. The auditor should conduct the engagement with a mindset that recognizes the possibility that a material misstatement due to fraud could be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity. Furthermore, professional skepticism requires an ongoing questioning of whether the information and evidence obtained suggest that a material misstatement due to fraud has occurred. In exercising professional skepticism in gathering and evaluating evidence, the*

[22] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, par. 76.

> *auditor should not be satisfied with less-than-persuasive evidence because of a belief that management is honest.*[23]

Professional skepticism requires an objective attitude toward the availability of evidence to sustain management's assertions—especially in areas that are more subjective, such as estimates of loss contingencies. The auditing standards have always required professional skepticism in the performance of an audit; however, in light of catastrophic business failures such as Enron, WorldCom, and Bernie Madoff's funds auditors are continuing to focus their efforts in this important area. The increased effort comports with SAS 99. Sarbanes-Oxley has much the same effect on management and boards: They, too, are called upon to exercise greater skepticism. (Professional skepticism is explored in more depth in Chapter 11.)

Knowledge and Experience

Auditors must deploy professionals with the necessary skills to perform an effective audit. Auditors should have a thorough understanding of the company and its industry or industries, and companies today often participate in widely different industries. For instance, a major retailer may have operations that include manufacturing and distribution and that also maintain a large portfolio of credit cards, which may require auditors to have skills in each of those three distinct businesses. Because every company is unique, auditors need to understand the important features of a company. Knowledge of a company and its complex and varied transactions is a cumulative endeavor. Forcing on companies a change of auditor in an effort to improve independence could run counter to this important ongoing need.

In addition to knowledge of the company and its industries, the audit team should have on hand individuals with the particular skills and expertise necessary to address myriad technical audit areas. Some of these are broad areas in which all auditors are knowledgeable, including auditing, internal control, and financial reporting. Others require specialized knowledge of forensic accounting, taxation, information technology, complex accounting, and financial reporting in such areas as derivatives and valuation and actuarial techniques.

Independence and Objectivity

Professional auditing standards require the auditor to maintain independence:

> *It is of utmost importance to the profession that the general public maintains confidence in the independence of independent auditors. Public confidence would be impaired by evidence that independence was actually lacking, and it might also be impaired by the existence of circumstances which reasonable people might believe likely to influence independence. To be independent, the auditor must be intellectually honest; to be recognized as independent, he*

[23] Id., par. 13.

> *must be free from any obligation to or interest in the client, its management, or its owners.*[24]

In January 2003, as required by the Sarbanes-Oxley Act of 2002, the SEC established independence rules governing auditors of SEC registrants. In those rules, the commission stated three basic principles of independence with respect to services provided by auditors, violations of which would impair the auditor's independence: auditors are not permitted to function in the role of management, auditors are not permitted to audit their own work, and auditors are not permitted to serve in an advocacy role for their client. (See Chapter 11 for a more detailed discussion of these rules.)

These general principles and the specific rules for carrying them out were established to enhance both the fact and the appearance of auditor independence. The critical reason for *being* independent is to help ensure that the auditor will think and act with objectivity; the critical reason for *appearing to be* independent is to inspire public trust with no ambiguity whatsoever.

SPADE

A framework that auditors may want to consider incorporates professional skepticism and several other elements that should be considered in the auditor's assessment of the risk of material misstatement caused by error or fraud:

S—Skepticism
P—Probing Communication
A—Analytics
D—Documentation
E—Evaluation

Skepticism stresses that the auditor must critically evaluate audit evidence and maintain a questioning mind, as described earlier. Probing communication involves inquiry and discussion with the audit team, company personnel, and the audit committee. While inquiry and discussion are not the only tools available to help the auditor obtain evidence, when inquiries are probing and incorporated with skepticism, the auditor is more likely to obtain the desired evidence. Analytics can provide excellent audit evidence in initial planning, scoping, validating, and audit completion. There are numerous types of analytics that can be performed, as well as tools that can be used to perform the analytics, and the auditor must be aware of these to use them most effectively. Documentation, which allows the auditor to describe the work performed and the basis for it, is a required duty of the auditor. It is the best means of allowing the proper assessment as to the execution of an audit response

[24] American Institute of Certified Public Accountants, AICPA Professional Standards—U.S. Auditing Standards—AU § 220, *Independence,* par. 3.

to risk and, furthermore, to determine if additional risk was identified during execution. Evaluation is essential in all phases of the audit, as it is the act of assessing the evidence obtained when taking into consideration other factors surrounding the company, such as the economy, industry, and internal controls.

Each of these elements is a powerful tool that the auditor should consider using throughout the audit.

AUDITING STANDARDS TAKE A RISK-BASED APPROACH TO FRAUD

Auditors are exposed to what is called *engagement risk,* which is the risk taken on by their professional practice due to its relationship with an engagement client. This risk might take the form of litigation, adverse publicity, lack of payment for the services performed, loss of professional reputation, or the loss of other clients. Engagement risk is also increased when the auditor has reservations about the integrity of management. Conversely, "engagement risk may exist even if there are no misstatements in the financial statements and the audit is conducted according to professional standards." For example, a client in poor financial condition presents engagement risk to the auditor based upon its likelihood of nonpayment or bankruptcy.[25] Engagement risk is usually assessed as part of the audit firm's client acceptance or continuance procedures. An auditor may decide that the risk of association with a client is so great that the engagement should not be undertaken, or the auditor may make the assessment that the engagement risk is within fully acceptable bounds and that the audit can, as a consequence, be planned and undertaken. Having decided to accept or continue the engagement, the auditor will then adopt a risk-based approach to planning and performing the audit.

The nature and characteristics of fraud have been discussed in Chapter 1, including the types of fraud relevant to the auditor and the conditions generally present when fraud occurs. (See also Chapters 22 and 23 on fraudulent schemes.) SAS 99 provides guidance for auditors concerning how to apply a risk-based approach to the possibility of fraud. The key guidelines are the following:

- *Discussion among engagement personnel regarding the risks of material misstatement due to fraud.* As part of planning the audit, there needs to be discussion among audit team members concerning how and where the entity's financial statements might be susceptible to material misstatement due to fraud. The discussion should reinforce the importance of adopting the mind-set of professional skepticism.
- *Obtaining the information needed to identify risks of material misstatement due to fraud.* The auditor must gather information needed to identify risks of material misstatement due to fraud. This is done by:
  - Inquiring of management and others within the entity about the risks of fraud: This inquiry encompasses information about alleged or suspected fraud,

[25] Larry E. Rittenberg and Bradley J. Schwieger, *Auditing: Concepts for a Changing Environment*, 4th ed. (Mason, OH: Thomson South-Western, 2003), 94.

knowledge of actual fraud, and management's views on the risk of fraud in the entity as well as about the programs and controls the company has established to mitigate specific, identified fraud risks.
  - Considering the results of the analytic procedures performed in planning the audit: Here the auditor's focus is on identifying unusual transactions and events as well as amounts, ratios, and trends that might indicate heightened risk of material misstatement due to fraudulent financial reporting.
  - Considering fraud risk factors: Here the auditor considers events or conditions that indicate incentives and pressures to perpetrate fraud, opportunities to carry out and conceal it, or attitudes and rationalizations that a fraudster might have in mind.
  - Considering certain other information, including results of the engagement team's fraud discussion, the auditor's client acceptance and continuance procedures, and information gained as a result of reviews of interim financial statements.
- *Identifying risks that may result in a material misstatement due to fraud.* The auditor uses the information gathered as described in the foregoing to identify risks that may result in a material misstatement due to fraud.
- *Assessing the identified risks after taking into account an evaluation of the entity's programs and controls.* The auditor evaluates the entity's programs and controls that address the identified risks of material misstatement due to fraud and assesses the risks in light of this evaluation.
- *Responding to the results of the assessment.* The auditor's response to the risks of material misstatement due to fraud involves the application of professional skepticism when gathering and evaluating audit evidence. The auditor considers responding to the results of the risk assessment in three ways:
  - A response that has an overall effect on how the audit is conducted—that is, a response involving general considerations apart from the specific procedures otherwise planned: This might involve the assignment of additional staff with specialized knowledge and skills to the engagement. Another example would be the decision to incorporate greater unpredictability in the selection of auditing procedures and locations to be audited from year to year.
  - A response to identified risks in terms of the nature, timing, and extent of the auditing procedures to be performed: Such procedures will vary depending on the types of risks identified and the account balances, classes of transactions, and related financial statement assertions that may be affected. The auditor may test the entity's controls designed to prevent and detect fraud, perform substantive auditing procedures, or use a combination of both.
  - A response involving the performance of certain procedures to further address the risk of material misstatement due to fraud involving management override of controls, as discussed in the next section.
- *Evaluating audit evidence.* Throughout the audit, the auditor must assess the risks of material misstatement due to fraud and must evaluate at the completion of the audit whether the accumulated results of auditing procedures and other observations affect the assessment. Furthermore, the auditor has to first consider whether identified misstatements may be indicative of fraud and then, if so, evaluate their implications.

MANAGEMENT OVERRIDE

Chapter 1 discussed the importance of management in the overall framework for fraud deterrence. Most often, management is part of the solution, but sometimes it is not just part of the problem but the source of the problem. Auditors face a dilemma with regard to their reliance on management: While they need management's cooperation to do the audit, management is in a position to mislead them in their gathering of evidence. Regarding controls over the quality of financial reporting and deterrence of fraud, this potential dilemma is particularly acute. On one hand, top management is responsible for fostering effective internal control throughout the organization. On the other hand, top management is in a unique position to perpetrate fraud because of its ability directly or indirectly to override established controls and enlist others in its efforts to do so.

Auditing standards have long recognized the possibility of management override as one of the limitations on the auditor's ability to rely on internal controls to prevent or detect misstatements. As a result, no matter how effective the auditor assesses the company's internal controls to be, the auditor generally performs substantive tests on significant account balances and classes of transactions. With regard to fraud, SAS 99 sets out three areas that require substantive procedures that specifically address the risk of management override: journal entries and other adjustments, accounting estimates, and significant unusual transactions.

Massive financial statement fraud often involves manipulation of the financial reporting process by the recording of inappropriate or unauthorized journal entries or by the adjusting of amounts reported in the financial statements that are not reflected in formal journal entries—for example, through consolidating adjustments, report combinations, and reclassifications. To specifically address this risk, SAS 99 requires the auditor to design procedures to test the appropriateness of journal entries recorded in the general ledger and of other adjustments made in the preparation of the financial statements.

As noted earlier in this chapter, significant estimates requiring management judgment have often been used as vehicles for committing fraud. To address this risk, SAS 99 instructs auditors to perform a retrospective review of past accounting estimates for biases that could result in material misstatement due to fraud. Such reviews are intended to afford auditors a look at management's past estimates, with the benefit of hindsight, so that they can identify management biases, if any, that might call into question the reasonableness of current estimates.

Fraud often involves the use of fictitious transactions or transactions whose sole or main purpose is to generate a particular financial result. Recognizing this, SAS 99 instructs auditors to gain an understanding of the business rationale for all significant transactions that fall outside the normal course of business or otherwise appear to be unusual, given the auditor's understanding of the entity and its environment.

REGULATORY REACTION TO FRAUD

Sarbanes-Oxley does not emphasize fraud per se, even though the Act originated out of corporate fraud scandals. Rather, it addresses the root of the problem by

addressing the framework for *effective* controls over financial reporting and other public disclosures. Section 302 requires the CEO and chief financial officer (CFO) to certify quarterly that the auditors and the audit committee have received notice of any fraud—*whether or not material*—involving management or others with a significant role in internal controls.

Signing officers—in addition to those within the organization who certify lower-level financial statements, thereby providing support for the CEO and CFO—are urged to fully understand the U.S. government's reasoning for the 302 provision. In previous frauds, the Department of Justice (DOJ) often became frustrated because it could not prove a nexus between the company's officers and the fraud. The officers would shrug their shoulders upon learning of the defalcation and claim that they had no knowledge of it. Since the enactment of 302, those days are gone: Section 302 specifically requires the CEO and CFO to take certain steps before they sign that one-page statement. Failure to do so now could land them in prison.

FINANCIAL BENEFITS OF EFFECTIVE FRAUD MANAGEMENT

Sarbanes-Oxley and SAS 99 demand that management, boards, and auditors pay closer attention to fraud. The good news is that effective fraud management is good for business. The Association of Certified Fraud Examiners reports that the average U.S. company loses the equivalent of *7 percent of revenue* to fraud and abuse. As discussed in Chapter 1, if 7 percent is applied to the estimated 2008 U.S. gross national product of $14.196 trillion, companies lost $994 billion to fraud in 2008. If these losses could be mitigated with effective fraud management, consider the impact of an additional 7 percent of revenue dropping to the bottom line. Most management teams would be very pleased with that degree of profit improvement.

CONCLUSION

For the foreseeable future, corporate fraud is likely to present substantial challenges to both auditors and forensic accounting investigators. Remembering the analogy of the patrol officer, we can recognize that auditing cannot realistically prevent financial reporting fraud or prevent employees from looting corporate assets. It may deter some fraud and detect others, but it is unlikely that auditors using the traditional audit concepts of selective testing (sampling) to obtain reasonable—not absolute—assurance that financial statements are fairly presented—not necessarily 100 percent accurate—will always identify material misstatements caused by fraud. As contemplated by SAS 99, auditing techniques and procedures can and will be improved, and future standards will likely institute further improvements. However, it must be recognized that the complexities of the business world and the ingenuity of highly educated white-collar criminals will always manage to produce schemes that unfortunately go undetected until they reach significant proportions. Forensic accounting investigators will investigate, prosecutors will convict, and regulators will react with new and more requirements. However, fraud will always persist.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 4

Auditor Responsibilities and the Law

Geoffrey Aronow and Hartwell Harris*

The pressure to establish increased auditor responsibility has been stronger in some decades and weaker in others. Recently, it has tended toward the former. The Sarbanes-Oxley Act of 2002 and its implementation are the latest steps in seeking to enhance the role of auditors in detecting and helping prevent financial fraud. There are lessons to be learned from a review of the past eight decades—lessons that can help identify potential future risks to auditors and strategies for minimizing those risks.

Over 75 years ago, Judge (later Justice) Benjamin Cardozo recognized, in the important *Ultramares* decision, the danger of exposing auditors to "a liability in an indeterminate amount for an indeterminate time to an indeterminate class" for "failure to detect a theft or forgery beneath the cover of deceptive entries"—in other words, management fraud.[1] Cardozo held that, under the rule of privity of contract (the relationship between contracting parties), only the audit client could sue accountants for negligent auditing and failing to detect a fraud. To allow other parties to sue on such grounds, Cardozo warned, would make the "hazards of a business conducted on these terms . . . so extreme as to enkindle doubt whether a flaw may not exist in the implication of a duty that exposes to these consequences."

Since then, with each wave of corporate scandals, reformers have pushed, often with some success, to enhance safeguards for investors, and implementation of those safeguards has fallen principally on the shoulders of the accounting profession. From one perspective, many of those measures were aimed at closing the so-called expectations gap between the auditor's legal responsibilities and the widespread public belief that the audit process should provide absolute assurance against financial fraud and misstatement. Moreover, through the years, new rules have sought to make it easier (but sometimes harder) in certain instances for people to

---

*Partner and Associate, respectively, at the law firm, Bingham McCutchen LLP. Andrew Karron and James Thomas, of Arnold and Porter LLP, served as co-authors with Mr. Aronow on a previous edition of this chapter, and much of their work continues to be reflected in its contents.

[1] *Ultramares Corp. v. Touche, Niven* and *Co.*, 255 N.Y. 170, 179; 174 N.E. 441, 444 (1931). The fraud in this case involved posting to the general ledger a fictitious entry of more than $700,000 in accounts receivable, thereby more than doubling the true amount of accounts receivable. See id., 443.

seek recovery from auditors for alleged injuries resulting from failures to detect management fraud or financial misstatement.

The modern practice of external auditing through selective testing dates to the early twentieth century. These early test audits examined not only internal company records of selected transactions but also evidence from outside sources about such transactions. The American Institute of Certified Public Accountants (AICPA) published the first authoritative auditing pronouncement in 1917 and revised it in 1929. Lenders increasingly began demanding audited financial statements as a basis for making credit decisions, and investors also began seeking audited financial data.

In that environment, Judge Cardozo handed down the *Ultramares* decision in 1931. That landmark decision can be understood as judicial recognition that audited financial statements have social value. Because audited financial statements are more reliable than unaudited financial statements, lenders and others are more willing to rely on them and to risk capital, which encourages investment. The lower risk associated with audited financial statements is reflected in a lower cost of capital. Judge Cardozo implicitly recognized that the cost of exposing auditors to "a liability in an indeterminate amount for an indeterminate time to an indeterminate class" might lead to abandonment of the field of auditing or to prohibitive audit fees that would reduce the frequency—and, as a consequence, the social utility—of audits. Thus, he found, any benefit to the plaintiff from a broad rule of liability would be vastly outweighed by the social costs of the loss of affordable financial statement audits.

Shortly after *Ultramares,* Congress recognized the social value of audits in the Securities Act of 1933 and the Securities Exchange Act of 1934. These laws, and the implementing regulations of the new Securities and Exchange Commission (SEC), required every public company to submit annual audited financial statements. Subsequently, government regulators of banks and other financial institutions followed suit.

The widespread adoption of requirements concerning audited financial statements led to the dramatic development of the profession. During the next 40 years, the AICPA published more than four dozen statements on auditing standards. Public accounting firms grew in size and scope and developed sophisticated training procedures and auditing systems. As audited financial statements became ubiquitous, public expectations about the effectiveness and significance of audits also grew.

Even the U.S. Supreme Court, in its important decision of 1984—*United States v. Arthur Young & Co.*—placed heavy emphasis on public responsibility and public trust in its discussion of the role of the auditor:

> *By certifying the public reports that collectively depict a corporation's financial status, the independent auditor assumes a public responsibility transcending any employment relationship with the client. The independent public accountant performing this special function owes ultimate allegiance to the corporation's creditors and stockholders, as well as to the investing public. This "public watchdog" function demands that the accountant maintain total independence from the client at all times and requires complete fidelity to the public trust.*[2]

[2] *United States v. Arthur Young & Co.*, 465 U.S. 805, 817–818 (1984).

Notwithstanding that the accounting profession and its authoritative literature continued to prescribe selective testing and concepts of "reasonable assurance"—implicit recognition that an audit might not detect all errors or fraud—users of financial statements increasingly treated audited financial statements as providing something more. Many in the public came to presume that audits should provide a virtual guarantee against fraud, a view that seems to persist to this day.

The National Commission on Fraudulent Financial Reporting, better known as the Treadway Commission, said in 1987 that users of audited financial statements "expect auditors to search for and detect material misstatements, whether intentional or unintentional, and to prevent the issuance of misleading financial statements." A survey in Canada from around the same time reported:

> *The public at large and even some quite sophisticated members of the financial community have only a vague understanding of the responsibilities undertaken and the work done by the auditor. To the public it is the end result, the financial disclosure, that is important. The auditor is quite likely to be the first to be blamed for errors or inadequacies in financial disclosure almost without regard to his or her audit responsibility.*[3]

The accounting profession has taken steps over the years to close the expectations gap by clarifying the respective responsibilities of management and auditors for financial statements. The standard audit opinion report was revised to state that the "financial statements are the responsibility of the Company's management" and that the auditors "express an opinion on these financial statements based on our audit."[4] Other participants in the corporate reporting process have sought to improve management's compliance with its obligations. For example, the Treadway Commission focused attention on best practices for corporate governance to improve financial reporting. The commission reiterated that the "public company has the initial and the final responsibility for its financial statements. Within the company lies the greatest potential for reducing fraudulent financial reporting."[5] Management controls the environment in which financial reporting takes place; notably, it develops and implements the internal controls over financial reporting. It will always be the case that company personnel in general and management in particular will have greater access to information and greater insights into the operations of the company than the outside auditor. Sarbanes-Oxley reinforced the role of corporate management by requiring that CEOs and chief financial officers of public companies certify the accuracy of their financial statements and other financial information in their companies' annual and quarterly reports.

---

[3] Canadian Institute of Chartered Accountants (CICA), *Report of the Commission to Study the Public's Expectations of Audits* (Toronto: 1988), 11.

[4] American Institute of Certified Public Accountants (AICPA), AICPA Professional Standards—U.S. Auditing Standards—AU § 508, *Reports on Audited Financial Statements,* ¶ .08 (2007).

[5] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Report of the National Commission on Fraudulent Financial Reporting,* Chap. 2, 31 (1987), available at www.coso.org/publications.

But the accounting profession knew that it had further work to do in clarifying its role. The profession addressed the expectations gap by revisiting the standards for detection of fraud. Reexamining the auditor's role in detecting fraud and reporting suspected illegal acts has been a recurrent theme in virtually all of the profession's periodic self-examinations in the past 30-plus years—from the Cohen Commission in 1977[6] through the Treadway Commission in 1987, the Special Report of the Public Oversight Board in 1993,[7] the report of the AICPA Special Committee on Financial Reporting in 1994,[8] and the Report of the Public Oversight Board Panel on Audit Effectiveness in 2000.[9]

The standard setters followed suit. In 1988, the Auditing Standards Board issued what came to be known as the expectations gap standards, which consisted of two standards that addressed auditors' responsibilities with regard to the detection of fraud and the reporting of illegal acts—Statement on Auditing Standards (SAS) Nos. 53 and 54. SAS 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities,* defined the auditor's responsibilities for detecting material misstatements in a financial statement audit, with the emphasis on factors indicating fraud. SAS 54, *Illegal Acts by Clients,* required heightened awareness of the possibility of illegal acts and required the auditor to report to the audit committee certain illegal acts that came to the auditor's attention in the course of the audit.

In 1997, SAS 82, *Consideration of Fraud in a Financial Statement Audit,* superseded SAS 53 and clarified the auditor's role in detecting client fraud by identifying certain fraud risk factors that the auditor should consider and assess in the course of an audit. SAS 82, in turn, was superseded by SAS 99, *Consideration of Fraud in a Financial Statement Audit,* which further refined the auditor's responsibility to assess the risk of financial statement fraud.

Each of these standards made clear that auditors must take certain steps designed to enhance the likelihood of detecting fraud. At the same time, the standards carefully reiterated that the auditor seeks to obtain only "reasonable assurance" as to whether fraud has occurred and that, given the nature of fraudulent conduct and the inherently limited nature of audit procedures, a proper audit may not detect fraud.

More recent examinations have also recognized the importance of the auditors' role in detecting fraud. In October 2006, the advisory committee on the auditing profession, appointed by U.S. Treasury Secretary Henry M. Paulson Jr., issued its Final Report of the Advisory Committee on the Auditing Profession to the U.S.

---

[6] American Institute of Certified Public Accountants (AICPA), Commission on Auditors' Responsibilities (Manuel F. Cohen, chairman), *Report, Conclusions and Recommendations* (1977).

[7] Public Oversight Board, *In the Public Interest—A Special Report* (1993).

[8] American Institute of Certified Public Accountants (AICPA), AICPA Special Committee on Financial Reporting, *Improving Business Reporting—A Customer Focus* (1994).

[9] Public Oversight Board, Panel on Audit Effectiveness, *Report and Recommendations* (2000), available at www.pobauditpanel.org/download.html.

Department of the Treasury.[10] In their opening statement, the co-chairs reiterated the important role that audits play in the capital markets:

> *Ultimately, it is a combination of transparency and trust that enables our financial markets to function efficiently. A strong and vibrant auditing profession is a critical element of that regime and especially important to the U.S. capital markets where more than 100 million people invest their savings and retirement assets.*

In this context, the subcommittee on firm structure and finance, "[r]ealizing the importance of the reliability of financial statements to investor confidence," focused on enhancing auditors' fraud detection capabilities.[11] The subcommittee issued seven recommendations to the SEC. Two of those recommendations directly addressed fraud prevention. In one recommendation, the subcommittee urged the SEC and Congress to empower the PCAOB to create a national center to facilitate the sharing of fraud prevention and detection experiences and best practices by auditing firms' and other market participants.[12]

In the other recommendation, the subcommittee urged the PCAOB to set standards that improve the auditor's standard reporting model and urged both the PCAOB and the SEC to clarify in the auditor's report the auditor's role in detecting fraud.[13] The subcommittee noted that the current report model does not actually mention fraud and is silent as to the auditor's responsibility to find fraud.[14] The subcommittee noted that testimony had revealed that there were differing views about what auditors are expected to discover. To date, neither the SEC nor the PCAOB has publicly stated whether they plan to implement these recommendations.

There are three main sources of guidance regarding the issue of fraud detection in the audit process: accounting standards developed by the profession, statutory enactments, and case law. Until Congress passed Sarbanes-Oxley, the accounting profession was largely self-regulated through AICPA. Sarbanes-Oxley granted the SEC the power to create the PCAOB—marking the end of the profession's self-regulation and the beginning of federal oversight of the accounting profession.

The PCAOB has adopted SAS 99 as part of its interim auditing standards.[15] SAS 99 instructs auditors to design and perform the audit to obtain reasonable assurance that the financial statements are free of material misstatements, whether caused by fraud or something else. SAS 99 offers guidelines for ways to plan and design an

---

[10] *Final Report of the Advisory Committee on the Auditing Profession to the United States Department of the Treasury* (October 2006), available at www.treas.gov/offices/domestic-finance/acap/docs/final-report.pdf.
[11] Id. at II: 4.
[12] Id. at Recommendation 1, VII: 2.
[13] Id. at Recommendation 5, VII: 13.
[14] Id. at VII: 15.
[15] Public Company Accounting Oversight Board (PCAOB), Interim Auditing Standard AU § 316.

audit to detect fraud. Notably, SAS 99 does not impose a direct responsibility on the auditor to investigate and detect fraud; rather, it offers ways for auditors to design their audits to better detect fraud.

Since its inception, the PCAOB has focused its energy on implementing new internal control standards and, with the exception of one committee meeting in 2004, has not considered the issue of the fraud detection standards—until very recently. Those more recent stirrings suggest that this issue may become a greater center of attention for the PCAOB in the future.

Back in 2004, the Standing Advisory Group (SAG) met to discuss issues relating to the detection of fraud. As a guide for discussion at that meeting, the office of the chief auditor issued a paper describing the current fraud detection regime.[16] The paper states: "SAS No. 99... still contains a considerable amount of discussion that primarily serves the purpose of disclaiming any responsibility on the part of auditors to detect fraud. This language focuses on a lack of responsibility rather than articulating a clear statement of responsibility that acknowledges the auditor's role of protecting public investors."[17]

Since the SAG meeting in 2004, the PCAOB has not taken any further action with regard to financial fraud, and the topic was not part of its formal standard-setting agenda for 2010. At an October 2009 SAG meeting, however, some SAG members voiced their concern about a need to revisit SAS 99 as a foundational standard.[18] Damon Silvers, associate general counsel, AFL-CIO, and a member of the Congressional oversight panel appointed by Congress for the Troubled Asset Relief Program, stated:

> *The overall fraud standard needs to be strengthened at the same time you undertake this exercise.... I think we need to move the dial a little bit so auditors have some greater obligation than is currently embodied in the current fraud standard, to have an obligation to act when there is reasonable suspicion of fraud.*

To similar effect, in the October 2006 final report of the advisory committee on the auditing profession to the U.S. Department of the Treasury, the committee recommended that the PCAOB, "in light of the continuing 'expectations gap,'" review the fraud detection and reporting standards.[19] In making this recommendation, the committee emphasized the public investor's expectations of the auditing profession: "Among the attributes that the public expects of auditors is a clear acknowledgment of their responsibility for the reliability of financial statements, particularly with respect to the detection of fraud, notwithstanding the

---

[16] Standing Advisory Group Meeting, *Financial Fraud* (September 8–9, 2004), available at www.pcaobus.org/Standards/Standing_Advisory_Group/Meetings/2004/09–08/Fraud.pdf.
[17] Id. at 7.
[18] Financial Reporting Blog, *PCAOB Announces Ambitious Agenda; May Be Time to 'Dial Up' on Fraud, Silvers Says* (October 14, 2009), available at http://financialexecutives.blogspot.com/2009/10/pcaob-announces-ambitious-agenda-may-be.html.
[19] Final Report, *supra,* VII: 12, VII: 18, available at www.treas.gov/offices/domestic-finance/acap/docs/final-report.pdf.

recognition that a company's management and board have the primary role in preventing fraud."[20]

For now, however, SAS 99 remains the fraud-detection standard in the profession.

Sarbanes-Oxley was not Congress's first foray into regulating the auditor's role in detecting and reporting fraud. In 1995, Congress passed Section 10A of the Private Securities Litigation Reform Act (PSLRA). Although the PSLRA, to a large extent, put in place requirements that had the effect of limiting the exposure of auditors to lawsuits, Section 301 of the legislation amended the Securities and Exchange Act to add a new Section 10A, which requires that audits of public company financial statements include "procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts."

Section 10A requires that an auditor who comes across information about an illegal act or strongly suggestive of it must "determine whether it is likely that an illegal act has occurred" and if so, "determine and consider the possible effect of the illegal act on the financial statements of the issuer." The auditor must then inform management and the audit committee of the illegal act. If the company's board fails to take remedial action, the auditor is required to take additional steps, up to and including resignation from the engagement and reporting the matter to the SEC.

This reporting requirement was a sea change for the profession; never before had auditors been required to report outside of the company they were auditing. The SEC has relied on Section 10A as a basis for enforcement actions against independent auditors.[21] In *SEC v. Solucorp Indus. Ltd.*,[22] the court held that, unlike Section 10(b) (the antifraud provision of the Securities Exchange Act), Section 10A does not contain a *scienter* requirement, and the SEC need not prove that an auditor acted knowingly or recklessly to establish a Section 10A violation. *In the Matter of David Decker, CPA, and Theodore Fricke, CPA,*[23] the SEC brought administrative proceedings under Exchange Act Section 21C and SEC Rule of Practice 102(e) against not only an audit partner but also an audit manager for failing to

---

[20] Id. at VII: 14 (urging that the PCAOB and the SEC clarify in the auditor's report the auditor's role in detecting fraud under the current auditing standards).

[21] *Grant Thornton LLP, et al.*, Admin. Proc. File No. 3-11377 (January 20, 2004); *In the Matter of Jeffrey M. Yonkers, CPA,* Admin. Proc. File No. 3-10354, AAER No. 1428 (July 27, 2001); *SEC v. Solucorp Indus. Ltd.*, 197 F. Supp.2d 4 (S.D. N.Y. 2002); *In the Matter of Charles K. Springer, CPA*, *Robert S. Haugen, CPA*, *Haugen, Springer and Co., PC,* Admin. Proc. File No. 3-10589, AAER No. 14*56 (September 27, 2001); *In the Matter of Aaron Chaitovsky, CPA*, *and Robert Glass*, *CPA,* Admin. Proc. File No. 3-10917, AAER No. 1652 (October 21, 2002); *In the Matter of David Decker, CPA, and Theodore Fricke, CPA,* Admin. Proc. File No. 3-11091, AAER No. 1762 (April 24, 2003); *In the Matter of Pat A. Rosetti, Admin.* Proc. File No. 3-10354 (May 2, 2001). See also *SEC v. KPMG, et al.*, Civ. Act. No. 03-CV-0671 (DLC) S.D. N.Y. (Complaint, Second Claim) (January 29, 2003); *SEC v. Chancellor Corp.*, 1:03-CV-10762, D. Mass. (Complaint, Twelfth Claim) (April 24, 2003).

[22] *SEC v. Solucorp Indus. Ltd.*, 197 F. Supp.2d 4 (S.D. N.Y. 2002).

[23] In the *Matter of David Decker, CPA, and Theodore Fricke, CPA,* Admin. Proc. File No. 311091, AAER No. 1762 (April 24, 2003).

discharge their responsibilities under Section 10A. Moreover, in a December 2000 speech to the AICPA, the SEC's then–director of enforcement, Richard H. Walker, asserted that an auditor's Section 10A responsibilities extend not only to illegal acts learned of in connection with year-end audit procedures but also to acts learned of by the auditor in connection with interim quarterly reviews of unaudited financial statements.[24]

In addition to agency enforcement actions, auditors are also potentially exposed to private litigation. Over the years, litigation involving auditors has produced decisions addressing fraud detection in the audit process. In some rulings in auditor liability cases, decisions at various times and in various circumstances (and jurisdictions), have reflected an expansive view of an auditor's role in the prevention and detection of fraud, notwithstanding SAS 99. Other courts, as well as legislatures on occasion, reflecting the concerns first voiced in *Ultramares,* have periodically enhanced protections for auditors against liability claims.

One of the U.S. Supreme Court's seminal decisions in this area, *Ernst and Ernst v. Hochfelder,*[25] reflects these competing considerations. The Court addressed the question of whether there was liability under Section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5 for negligent conduct, or whether a plaintiff needed to prove *scienter,* "a mental state embracing intent to deceive, manipulate, or defraud."[26] On the one hand, the Court held that proof of negligence was insufficient to impose liability. Rather, the Court held that a violation required *scienter*. On the other hand, the Court also said that in "certain areas of the law, recklessness is considered to be a form of intentional conduct for purposes of imposing liability."[27] The Court explicitly declined to address whether proof of "recklessness" could suffice to support liability under Section 10(b) and Rule 10b-5, and, since then, the Court has never directly addressed the issue.

Since that Supreme Court ruling, courts have uniformly accepted recklessness as sufficient to support auditor liability.[28] While various rulings have emphasized that recklessness should be understood as a "lesser form of intent," not a "heightened form of ordinary negligence,"[29] it is nonetheless true that a recklessness standard permits more cases to survive dismissal than would be the case if liability were confined to truly intentional conduct. And once a case goes before a jury, anything can happen. It should be noted, however, that the majority standard for

---

[24] See also *In the Matter of Seidelman, CPA*, AAE Rel. No. 2078 (August 11, 2004) (holding that failure to file a 10-Q with required financial information is an illegal act).
[25] *Ernst and Ernst v. Hochfelder,* 425 U.S. 185 (1976).
[26] Id. at 215.
[27] Id.
[28] See, for example, *Greebel v. FTP Software, Inc.*, 194 F.3d 185, 198–200 (1st Cir. 1999); *Press v. Chemical Inv. Servs. Corp.*, 166 F.3d 529, 538 (2d Cir. 1999); *Helwig v. Vencor,* 251 F.3d 540 (6th Cir. 2001); *City of Philadelphia v. Fleming Cos.*, 264 F.3d 1245, 1259 (3d Cir. 2001).
[29] See, for example, *SEC v. Steadman*, 967 F.2d 636, 641–42 (D.C. Cir. 1992); *Greebel,* 194 F.3d, at 199.

auditor liability in Rule 10b-5 cases defines *recklessness* to mean essentially no audit at all.[30]

At the same time, the law governing negligence claims under state or common law has evolved in certain jurisdictions to expose the auditor to substantially greater risk of liability than under the strict privity standard that New York State's highest court articulated in *Ultramares*. The high-water mark of expansive liability was probably reached in 1983, with the New Jersey Supreme Court's decision in *H. Rosenblum, Inc. v. Adler*.[31] There, the court rushed past *Ultramares* and held that auditors could be liable to any user of the financial statements for reasonably foreseeable negligence.

The bases for that decision provide important insights into the perceptions some have of the auditor's role, which underlie much of the persistent pressure toward imposing greater responsibility—and therefore greater liability when things go wrong. In reaching its conclusion, the *Rosenblum* court asserted that "accountability has clearly been the social and organizational backbone of accounting for centuries. . . . Accountability is what distinguishes accounting from other information systems in an organization or in a society." On the issue of fraud detection, the court conceded that the auditors will not "always be able to discover material fraud," but asserted that "the independent auditor should be expected to detect illegal or improper acts that would be uncovered in the exercise of normal professional skill and care." Almost wistfully, the court declared that "the audit, particularly when it uncovers fraud, dishonesty, or some other illegal act, serves an undeniably beneficial public purpose." The New Jersey court also dismissed practical concerns about the potential for "financial catastrophe" that had motivated the court in *Ultramares,* suggesting that accounting firms would be able to "purchase malpractice insurance policies that cover their negligent acts" and that increasing their liabilities would "cause accounting firms to engage in more thorough reviews."

Nine years later, in *Bily v. Arthur Young & Co.*,[32] the California Supreme Court expressly rejected the *Rosenblum* "foreseeability" standard, stating that it subjected auditors to unreasonable exposure. Rather, the court concluded, "an auditor owes no general duty of care regarding the conduct of an audit to persons other than the client."[33] The court held that an auditor could be liable to those "who act in reliance upon those misrepresentations in a transaction which the auditor intended to influence," which the court said was consistent with the standard set forth in the

[30] "Scienter requires more than a misapplication of accounting principles. The plaintiff must prove that the accounting practices were so deficient that the audit amounted to no audit at all, or an egregious refusal to see the obvious, or to investigate the doubtful, or that the accounting judgments which were made were such that no reasonable accountant would have made the same decisions if confronted with the same facts." In re *Software Toolworks Inc.*, 50 F.3d 615, 628 (9th Cir. 1994) (internal quotation omitted).
[31] *H. Rosenblum, Inc. v. Adler,* 93 N.J. 324, 461 A.2d 138, (1983), 461 A.2d 138 (N.J. 1983).
[32] *Bily v. Arthur Young & Co.*, 3 Cal. 4th 370, 11 Cal. Rptr. 2d 51, 834 P.2d 745 (1992), 834 P.2d 745 (Cal. 1992).
[33] Id. at 747.

Restatement (Second) of Torts.[34] In reaching that decision, the court said that an audit requires "a high degree of professional skill and judgment" and is

> *a professional opinion based on numerous and complex factors. . . . The report is based on the auditor's interpretation and application of hundreds of professional standards, many of which are broadly phrased and readily subject to different constructions. . . . Using different initial assumptions and approaches, different sampling techniques and the wisdom of 20-20 hindsight, few CPA audits would be immune from criticism.*[35]

In what has become a renowned phrase, the California court asserted that an "auditor is a watchdog, not a bloodhound."[36]

In a way seldom duplicated in recent years, the ruling recognized and took account of the reality of the dynamics of litigation:

> *Although the auditor's role in the financial reporting process is secondary and the subject of complex professional judgment, the liability it faces in a negligence suit by a third party is primary and personal and can be massive. The client, its promoters, and its managers have generally left the scene, headed in most cases for government-supervised liquidation or the bankruptcy court. The auditor has now assumed center stage as the remaining solvent defendant and is faced with a claim for all sums of money ever loaned to or invested in the client. . . . Although hindsight suggests [the plaintiffs] misjudged a number of major factors (including, at a minimum, the product, the market, the competition, and the company's manufacturing capacity), plaintiffs' litigation-focused attention is now exclusively on the auditor and its report.*[37]

The court reasoned that responsibility is more properly allocated in a much different manner:

> *As a matter of economic and social policy, third parties should be encouraged to rely on their own prudence, diligence, and contracting power, as well as other informational tools. . . . If, instead, third parties are simply permitted to recover from the auditor for mistakes in the client's financial statements, the auditor becomes, in effect, an insurer of not only the financial statements, but of bad loans and investments in general.*[38]

Finally, the court rejected the notion, embraced by the New Jersey Supreme Court in *Rosenblum,* that imposing liability on auditors would create an incentive to do better work.

---

[34] Id. at 770.
[35] Id. at 763.
[36] Id.
[37] Id. at 764.
[38] Id. at 765.

Since then, most jurisdictions have rejected, by court decision or by statute, New Jersey's broad foreseeability approach—including New Jersey itself, which enacted a statute overturning the *Rosenblum* decision.[39] Most states that have addressed the issue have adopted some form of the rule set forth in the Restatement (Second) of Torts. The Restatement standard essentially provides that "a supplier of information is liable for negligence to a third party only if he or she intends to supply the information for the benefit of one or more third parties in a specific transaction or type of transaction identified to the supplier."[40]

The public scandals of the last decade involving alleged and proven accounting improprieties may be the harbinger of heightened exposure. Some courts have been less attuned to limiting auditor liability and have taken an approach that focuses once again on such themes as the importance of audited financial statements in modern society and the gravity of the duty assumed by auditors of those financial statements. For example, in reversing the dismissal of a fraud claim by a lower court, the Appellate Division of the New York Supreme Court wrote:

> *Keeping in mind the difficulty of establishing in a pleading exactly what the accounting firm knew when certifying its client's financial statements, it should be sufficient that the complaint contains* some rational basis *for inferring that the alleged misrepresentation was knowingly made.* Indeed, to require anything beyond that would be particularly undesirable at this time, *when it has been widely acknowledged that our society is experiencing a proliferation of frauds perpetrated by officers of large corporations, for their own personal gain, unchecked by the "impartial" auditors they hired.*[41]

Liability actions based on allegations that an auditor failed to detect fraud can arise through regulatory action or private litigation. The SEC and the PCAOB regulate the auditing profession. Under the federal securities laws, the SEC has enforcement authority over public company auditing firms and, under Sarbanes-Oxley, has oversight authority over the PCAOB. Sarbanes-Oxley provides the PCAOB with registration, reporting, inspection, standard-setting, and enforcement authority over public company auditing firms.[42]

The PCAOB is tasked with enforcing SAS 99. Section 105 of Sarbanes-Oxley grants the PCAOB broad investigative and disciplinary authority over registered public accounting firms and persons associated with such firms. The PCAOB adopted

---

[39] See Carl Pacini, *et al.*, "At the Interface of Law and Accounting," *American Business Law Journal* 37 (Academy of Legal Studies in Business, 2000), 171, 175–179; see also *Dickerson & Son, Inc. v. Ernst & Young, LLP,* 2004 WL 963944 (N.J. May 6, 2004) (construing New Jersey statute to bar a claim against an accounting firm).

[40] See *Bily,* 834 P.2d at 758.

[41] *Houbigant, Inc. v. Deloitte & Touche LLP,* 753 N.Y.S.2d 493, 498 (N.Y. App. Div. 2003) [emphasis added].

[42] Sarbanes-Oxley Act of 2002, 15 U.S.C. Sections 7211–7219.

rules relating to investigations and adjudications in 2003, which the SEC subsequently approved in 2004.[43]

These rules enable the PCAOB to conduct investigations of registered public accounting firms and persons associated with such firms, or both. The rules grant the PCAOB investigative power to investigate acts, practices, or omissions that violate Sarbanes-Oxley, the PCAOB's rules, the securities laws relating to preparation of audit reports, and standards that govern the liability and obligations of accountants with respect to audit reports, including SEC rules and professional standards. When violations are detected, the PCAOB conducts a hearing and, in appropriate cases, imposes sanctions that are supposed to be designed to deter a possible recurrence and to enhance the quality and reliability of future audits. The sanctions may be as severe as revoking a firm's registration or barring a person from participating in audits of public companies. Lesser sanctions include monetary penalties and requirements for remedial measures, such as training, new quality control procedures, and the appointment of an independent monitor.[44]

To date, the PCAOB has issued 25 orders instituting disciplinary proceedings, making findings and imposing sanctions (Order).[45] Of those 25, nine Orders cited a failure to follow SAS 99[46] as one of the reasons for PCAOB action, and three Orders cited a failure to follow Section 10A. (One Order cited both.) The nature of the violations of SAS 99 and Section 10A that the board has found has varied. The severity of the penalties has also varied substantially. (A chart summarizing the 11 PCAOB actions that have cited SAS 99 or Section 10A appears at the end of this chapter.)

In addition to facing penalties imposed by the PCAOB, the SEC still retains its power to enforce Section 10A. Since the enactment of Section 10A in 1995, the SEC has taken an aggressive position in enforcing violations and shows no sign of changing course.[47] For violations of 10A, the SEC can proceed against auditors either in federal court or in a cease-and-desist administrative proceeding.

The SEC has imposed money penalties and barred individual auditors from practicing before the SEC for one, five, and ten years. The SEC has mainly imposed practice bars against individuals and firms that are not at the largest firms—the so-called Big Four. Because of the wording of the language of Section 10A, the SEC or the PCAOB can impose penalties only for violations of failures to report *out* to the SEC, and not failures to report *up* to the audit committee.[48]

---

[43] Public Company Accounting Oversight Board, Rules on Investigations and Adjudications (PCAOB Release No. 2003-015), (September 29, 2003), available at www.pcaobus.org/Rules/Docket_005/Release2003–015.pdf.

[44] See www.pcaobus.org/Enforcement/index.aspx.

[45] Public Company Accounting Oversight Board, Rules on Investigations and Adjudications (PCAOB) Release No. 2003-015 (September 29, 2003), available at www.pcaobus.org/Rules/Docket_005/Release2003–015.pdf.

[46] SAS 99 is codified in the PCAOB Rules as AU 316. For consistency, this chapter will refer to it as SAS 99.

[47] John Eickemeyer, "SEC Actions Against Accountants Under Section 10A of the Exchange Act," *Review of Securities and Commodities Regulation* 39(7): 56 (April 5, 2006).

[48] See *In the Matter of Gary L. Seidelman, CPA,* AAE Rel. No. 2078 (August 11, 2004) (individual auditor cited for failure to determine whether an act was an "illegal act" but no civil penalty imposed because a failure to report to the SEC was not at issue).

In addition to liability imposed by regulators, auditors also face potential liability in civil litigation. The number of securities fraud cases initially involving auditors has steadily decreased since 2002; auditors were named in 2 percent of securities litigation cases in 2008, down from 6 percent in 2002.[49] One possible explanation is that the PSLRA and subsequent judicial interpretations of the Act have made it more difficult to allege fraud violations against auditors. But caution must be taken with regard to this statistic, since it is based solely on examination of initial complaints in a case. The heightened pleading requirements of the PSLRA have made class action plaintiffs' attorneys more reticent to name auditors right at the beginning of litigation. But it is likely that auditors are being added as defendants later in the actions, when the plaintiffs may feel they have developed sufficient evidence through discovery to survive a motion to dismiss. And the percentage of cases in which that presents a real possibility continues to rise: In 2008, 94 percent of the cases involved allegations of misrepresentations in financial documents (up from 82 percent in 2002).[50]

Allegations of fraud have decreased from 91 percent in 2003 to 75 percent in 2008. This statistic may also be misleadingly reassuring, since allegations of violations of Section 11 of the Securities Act of 1933[51] have increased from a low of 7 percent in 2004 to 23 percent in 2008. This is significant, because, when alleged independently of fraud claims, Section 11 does not require allegations of scienter. It is easier for plaintiffs to get past the pleading stage when alleging Section 11 claims. Moreover, while Section 11 allows for a due diligence defense, such a defense is a realistic tool only at trial; it cannot help to weed out baseless allegations in earlier stages of litigation. The result may well be higher litigation costs and risks for auditors.

While the number of cases against auditors may have decreased, median settlement amounts have varied slightly over the past few years and have remained quite substantial. In 2008, the median settlement amount was $7.5 million, $9.4 million in 2007, and $7.0 million in 2006.[52]

Averages and medians, moreover, tend to obscure the degree of risk: The exposure in these cases can be staggering. Auditors have paid large settlements in several recent cases: $335 million to settle claims arising from audits of Cendant Corporation; $125 million to settle claims arising from audits of Rite-Aid Corporation; and $110 million to settle claims arising from audits of Sunbeam Corporation.[53] From 1995 through 2007, the six largest accounting firms paid out $3.68 billion to resolve

---

[49] Cornerstone Research, *Securities Class Action Filings, 2008: A Year In Review* (New York: Cornerstone Research, 2009), 22.

[50] Id. Interestingly enough, complaints alleging GAAP violations dropped during the period of 2002 to 2008, from 58 percent to 44 percent. *Id*.

[51] 15 U.S.C. § 77k.

[52] NERA Economic Consulting, *2008 Trends in Securities Class Actions,* available at www.nera.com/image/PUB_Recent_Trends_Report_1208.pdf

[53] Auditors face increased pressure from regulators as well. In early 2004, an SEC administrative law judge imposed on Ernst & Young LLP a six-month bar from accepting new public company audit clients as a sanction for violations of the independence requirements—even though there was no allegation or proof of any audit failure or financial statement misstatement by Ernst & Young's client. See *In the Matter of Ernst & Young LLP,* Administrative Proceeding File No. 310933 (ALJ April 16, 2004).

cases related to public company audits.[54] This represents 65 percent of the total paid out to resolve 362 cases related to public company audits as well as private company audits and nonaudit services.[55] The weighted average of litigation and protection costs for these firms was 6.6 percent of revenues and 15.1 percent of audit-related revenues.[56]

* * *

Yogi Berra once said, "It's tough to make predictions, especially about the future." Nonetheless, it seems safe to predict that many among the investing public and government officials will seek to impose high standards of accountability on auditors. Ironically, efforts to respond to those expectations by enhancing audit procedures risk raising expectations—and the accompanying risk of litigation—even higher.

One likely result of the additional requirements imposed by Sarbanes-Oxley and the PCAOB is the increase in the cost of audits. This has already occurred, particularly as a result of Sarbanes-Oxley's and the PCAOB's controversial requirement for reports by companies and attestation reports by auditors on the internal controls of public companies.[57]

As the major firms are effectively self-insured because the cost of insurance is prohibitive, the risks associated with audits of new and innovative businesses may be viewed as creating unacceptable risks to those firms that can afford to pick and choose their clients. The result may be that such companies will not be able to retain the most sophisticated and most experienced accounting firms. There is some indication that this has happened to a degree, in part due to the resources needed to comply with the requirement for reports on internal controls.[58] Thus, in attempting to preserve the social utility of financial statement audits, the enhanced regulatory framework ultimately may have the opposite effect—at least in some parts of the economy.

Auditors cannot become guarantors of corporate integrity, which remains the responsibility of the company and its board. To the extent that enhanced fraud auditing procedures are implemented, however, they may assist corporate management and boards in discharging their duties.

---

[54] Final Report, *supra,* p. VII: 25, available at www.treas.gov/offices/domestic-finance/acap/docs/final-report.pdf.
[55] Id.
[56] Id. at VII: 26.
[57] See, for example, Deborah Solomon and Cassell Bryan-Low, "Companies Complain about Cost of Corporate-Governance Rules," *New York Times,* February 10, 2004 (noting 30 percent increase in audit costs); see also "Auditing Standard No. 2—An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" (Public Company Accounting Oversight Board, March 9, 2004), www.pcaobus.com/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_2.pdf.
[58] Auditing Standard No. 2, *supra.* Sarbanes-Oxley's and the PCAOB's requirements relating to the documentation of audits may also spur this trend. See also Auditing Standard No. 3 (AS3)—*Audit Documentation* (PCAOB: June 9, 2004), available at www.pcaobus.com/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_3.pdf.

APPENDIX: SUMMARY OF PCAOB MATTERS INVOLVING DETECTION OF FRAUD

Matter	Fraud Violations	Penalties
Lawrence Scharfman CPA PA, and Lawrence Scharfman, CPA (8/11/2009)	Section 10A: Failure to act after becoming aware of illegal acts and violation of independent requirements SAS 99/AU 316: Failure to conduct a retrospective review of reserve	Firm: Registration revoked Individual: Barred from being an associated person of a registered public accounting firm
Thomas J. Linden, CPA (8/11/2009)	SAS 99/AU 316: Failure to respond to last-minute adjustments	Individual: Barred from being an associated person of a registered public accounting firm and fined $75,000
Christopher E. Anderson, CPA (10/31/2008)	SAS 99/AU 316: Failure to consider last-minute adjustments	Individual: Suspension from being associated with a registered public accounting firm for one year; restriction to the role of assistant, for an additional year; and fined $25,000
Jaspers + Hall, PC, Thomas M. Jaspers, CPA, and Patrick A. Hall, CPA (10/21/2008)	SAS 99/AU 316: Failure to gain an understanding of the business rationale for transactions outside the normal course of business or that otherwise appear unusual	Firm: Registration revoked Individuals: Barred from being associated person of a registered public accounting firm
Kantor, Geisler & Oppenheimer, P.A., Steven M. Kantor, CPA, and Thomas E. Sewell (12/14/2007)	Section 10A: Failure to determine likelihood of illegal act and performance of prohibited services	Firm: Registration revoked Individuals: Barred from being associated persons of a registered public accounting firm indefinitely and for one year
James L. Fazio, CPA (12/10/2007)	SAS 99/AU 316: For failure to conduct a retrospective review of reserve	Individuals: Barred from being associated person of a registered public accounting firm
Deloitte & Touche LLP (12/10/2007)	SAS 99/AU 316: Failure to evaluate the reasonableness of estimates of future returns and to compare these to historic returns	Firm: Censured, fined $1,000,000, and forced to undertake certain actions

(*Continued*)

Matter	Fraud Violations	Penalties
Thomas Benson and Thomas Benson, CPA (6/29/2007)	SAS 99/AU 316: Failure to respond to indicators of risk	Firm: Registration revoked Individual: Barred from being associated person of a registered public accounting firm
Armando C. Ibarra, P.C., Armando C. Ibarra, Sr., and Armando C. Ibarra, Jr. (12/19/2006)	SAS 99/AU 316: Failure to perform and/or document a discussion among engagement personnel regarding the risk of material misstatement due to fraud	Firm: Registration revoked Individuals: Barred from being associated person of a registered public accounting firm
Turner Stone & Company, LLP, and Edward Turner, CPA (12/19/2006)	SAS 99/AU 316: Failure to respond to indicators of risk	Firm: Censured Individual: Barred from being associated person of a registered public accounting firm

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 5

When and Why to Call in Forensic Accounting Investigators

Darren J. Tapp and W. McKay (Mac) Henderson

Chapter 3 discusses the many differences between the work of the forensic accounting investigator and the work of the financial statement auditor. A key question in any audit that identifies indicia of possible fraud is: When should the auditor, external or internal, consider reaching out for the forensic accounting investigator? Determining that *when* is the focus of this chapter.

Many forensic accounting investigators would take the position that the typical financial statement auditor may wait too long before calling in the forensic accounting investigator. But no savvy auditor reading these words will fail to notice the possibility of bias in the statement; after all, this book is written by a team of forensic accounting investigators. And so, part of the aim of this chapter is to demonstrate that the decision regarding when to call in the forensic accounting investigator can and must be viewed in an objective light. Before proceeding further, readers might find it helpful to review Chapter 1, in which we introduced the concept of using forensic accounting investigators on audits when suspicions arise.

The thoughtful and efficient use of forensic accounting investigators often offers the right balance between conducting routine audits and investigating for possible fraud. A predicate must exist before an investigation is undertaken. A *predicate* is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, or will occur. Predication is the basis for undertaking a fraud investigation.[1] It would be inappropriate—and a violation of the Association of Certified Fraud Examiners' (ACFE) standards of professional conduct—to begin an investigation without sufficient predication.

Some auditors may call in forensic accounting investigators at the slightest suspicion of fraud. Year after year, they may bring in these forensic accounting investigators at the same client; their mind-set is to consult early and often—not only with

[1] Association of Certified Fraud Examiners, CFE Code of Professional Standards, IV. Standards of Examination § A.2: "Members shall establish predication and scope priorities at the outset of a fraud examination and continuously reevaluate them as the examination proceeds. . . ."

forensic accounting investigators but also with industry experts and the risk-and-quality auditors who typically provide, from the center of major accounting firms, an internal consulting service for audit teams in the field. Auditors who rely on forensic accounting investigators at the first sign of possible fraud usually recognize that the skill set of fraud accountants differs from their own. Just like the actuary called in to evaluate the pension benefit accrual or the tax specialist who reviews the tax accrual, the forensic accounting investigator brings the experience and training required to properly evaluate suspicions of fraud. In our perhaps biased view, at the very first sign of fraud, consideration should be given to bringing in the forensic accounting investigator to evaluate.

At the other extreme are auditors who believe they possess the know-how to conduct forensic investigations but they may not have trained, or trained sufficiently in the field, and certainly lack sufficient experience to meet the circumstances that may arise as an investigation develops. When they grow suspicious of fraud, they often test, they often inquire, they often engage in extended procedures, they often inquire further—but they may be confronted with ambiguous results from using further audit procedures based on sampling; or worse, they may reach erroneous conclusions. Requesting a forensic accounting investigation designed to resolve the suspicion of fraud may be appropriate.

TODAY'S AUDITORS ARE NOT FORENSIC ACCOUNTING INVESTIGATORS

Many outside the profession believe auditors have received extensive training in the skills of forensic accounting investigation. This is not so for most auditors. Undergraduate accounting programs do not, to the best of our knowledge, require courses in forensic accounting investigation, although some offer elective courses. The authors of this book are not suggesting that auditors be trained as forensic accounting investigators for all the reasons we have addressed, but principally because the discipline of forensic accounting investigation is an art requiring a different set of skills, training, education, and experience. What we expect to evolve in the education of future accountants is a curriculum that increases students' awareness of detection techniques as well as instruction that enables them to have an appreciation for the capabilities of forensic accounting investigators. In this way, these accounting graduates—whether they find their place in the business world in operations, management, or internal audit or as independent auditors—will better know the footprints of fraud and when to call upon the forensic accounting investigators, as is illustrated in Exhibit 5.1.

AUDITORS ARE NOT AUTHENTICATORS

Auditors are not responsible for detecting counterfeit documents. Any respectable fraudster with access to a color printer or copier can create a false paper trail that would deceive even an experienced auditor. We've seen situations in which entire sets of documents had been created—in some cases, overnight—to deceive auditors. Audits involve the review of tens of thousands of documents by auditors

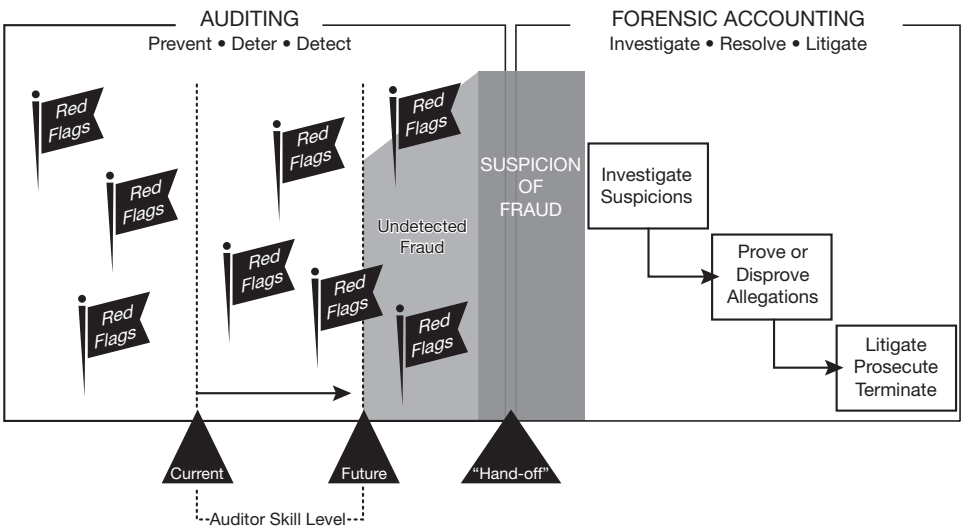


EXHIBIT 5.1 The Red Flags of Possible Fraud: When to Hand Off to Forensic Accounting Investigators

who are not routinely trained or necessarily experienced in spotting altered or forged documents. The auditor's professional standards do not hold auditors responsible for detection if a fraud is concealed by fraudulent documents. However, auditors armed with a healthy dose of skepticism will question the source from which they obtain information, recognizing that that information could be fraudulent.

AUDITORS HAVE LIMITED EXPOSURE TO FRAUD

Nothing short of repeated exposure to fraud can prepare one for effectively investigating frauds. Those who go on to become specialized forensic accounting investigators develop a keen sixth sense that supports the set of skills required for the resolution of complex fraud schemes.

When forensic accounting investigators launch a fraud investigation in an environment in which the perpetrator is unknown, they usually begin with interviews numerous enough to identify possible targets. During that process, they often hear such comments as: "Oh, it can't be Kathy. Kathy is one of our most loyal, long-term employees. She rarely takes time off, always works late, and helps others with their jobs. She's friendly, religious . . ." and so on. Such a commentary on Kathy's work ethic and personality has no impact on the forensic accounting investigator's attitude, which must remain one of professional skepticism. The great majority of friendly, hardworking employees are honest; they are what they seem. However, most fraudsters also seem to be honest. The word *con* is a shortened form of the word *confidence*. Fraudsters seek to gain one's confidence, and the best of them are very good at it.

No book or school can adequately teach these realities to anyone. No standard requiring professional skepticism can substitute for actual experience with deceit. Providing training to surface more indicia of fraud and having forensic accounting investigators to call upon when such evidence surfaces are the best solutions to the problem. However, not all frauds will be detected or investigated to their ultimate resolution.

AUDITORS ARE NOT GUARANTORS

For most of the past century, many participants in business—as well as some courts that adjudicated business disputes—believed that the auditor certified a company's financial statements, thereby becoming the guarantor of those statements' accuracy and reliability. However, in the mid-1980s that understanding of the auditor's responsibility changed dramatically with the Treadway Commission report.[2] The commission found that responsibility for reliable financial reporting resides "first and foremost at the corporate level." The commission defined the auditors' role as "crucial but secondary" and explicitly stated that the outside auditors' role was not that of "guarantors of the accuracy or the reliability of financial statements."

Later, in accountant liability litigation, the courts began to reshape their view of the auditor's role. Notably, in *Bily v. Arthur Young & Co.*—a decision cited earlier in this book—the judge wrote as follows:

> *An auditor is a watchdog, not a bloodhound. . . . As a matter of commercial reality, audits are performed in a client-controlled environment. The client typically prepares its own financial statements; it has direct control over and assumes primary responsibility for their contents. . . . The client engages the auditor, pays for the audit, and communicates with audit personnel throughout the engagement. Because the auditor cannot, in the time available, become an expert in the client's business and record-keeping systems, the client necessarily furnishes the information base for the audit. Thus, regardless of the efforts of the auditor, the client retains effective primary control of the financial reporting process.*[3]

No doubt the investing public and others who rely on financial statements have been frustrated over the issue of fraud detection. Who can blame them? However, those who rely on financial statements cannot get what they want by asking auditors to defy "commercial reality," as the judge brilliantly explains. As the public has clearly shown an interest in influencing all of those involved in the corporate

---

[2] Commonly referred to as the Treadway Commission, because it was chaired by James C. Treadway Jr., a former commissioner of the U.S. Securities and Exchange Commission, the body's actual name was the National Commission on Fraudulent Financial Reporting. Its task was to investigate the underlying cause of fraudulent financial reporting, analyze the role of the outside auditor, and focus on the corporate structure and its possible effect on fraudulent financial reporting.

[3] *Bily v. Arthur Young & Co.*, 3 Cal. 4th 370, 11 Cal. Rptr. 2d 51, 834 P.2d 745 (1992).

reporting chain to improve accountability and performance, there must be a greater appreciation for the skills of forensic accounting investigators.

HISTORICALLY, AUDITS MAY HAVE BEEN PREDICTABLE

Many have suggested that the reason auditors did not detect in a timely manner the fraudulent schemes leading to some of the more significant corporate scandals was simply that the auditors' audit procedures had become predictable. There is no secret about what well-trained auditors examine in the course of an audit performed in accordance with Generally Accepted Auditing Standards (GAAS). Once the audit leader has identified the risk areas in a financial statement prepared by company management, the focus and scope of the planned audit are defined easily enough. However, the relatively routine, predictable character of audit planning creates opportunities for fraud. When it is easy to determine the scope of an audit, it is often easy to plan a fraud around it.

> Predictability of auditing procedures. *The auditor should incorporate an element of unpredictability in the selection from year to year of auditing procedures to be performed—for example, performing substantive tests of selected account balances and assertions not otherwise tested due to their materiality or risk, adjusting the timing of testing from that otherwise expected, using differing sampling methods, and performing procedures at different locations or at locations on an unannounced basis.*[4]

The landscape has changed rapidly for financial statement auditors. Arthur Andersen collapsed in the aftermath of the Enron scandal; a major health care provider has been accused of fabricating documents to deceive its auditors as part of a scheme to increase revenues; and other instances of accounting and audit abuse continue to emerge.

Auditors allegedly have been placed on the front line in the battle against fraud. They face the public and regulatory expectation that they will play a key and continuing role in restoring the integrity of financial reporting. This message is embedded not only in the language of Sarbanes-Oxley, but also in the Public Company Accounting Oversight Board (PCAOB) modifications of the standards governing quality control and the independence standards and the rules that provide the framework for the audit, which are in process. These are discussed in Chapter 11.

As noted in earlier chapters, the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) No. 99 outlines procedures the auditor must follow in assessing the potential risk of fraud and the impact on financial statement reporting. This standard became effective for audits of financial statements for periods beginning on or after December 15, 2002. Among its many topics, SAS 99

[4] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par. 50.

highlights the need to bring in subject matter experts (SMEs)[5] to assist the audit team or to investigate allegations or indications of fraud. To forensic accounting investigators, the thought process outlined by SAS 99 is just another chapter in a lifetime's work of ferreting out fraud schemes and corporate misconduct through the use of tried-and-true techniques. Forensic accounting investigators can bring such skills and experience to any stage of the audit.

POTENTIAL TRIGGER POINTS OF FRAUD

- *Anonymous allegations of fraud, whether by letter, e-mail, hotline, or anonymous call.* Whistle-blowers should be treated with utmost care. While seeking to take the allegations seriously, companies may wait too long to respond to whistle-blowers, who then believe they're not being taken seriously and who make a phone call to a third party such as the U.S. Securities and Exchange Commission (SEC) or the media. Every effort should be taken to respond to whistle-blowers immediately. Whistle-blowers should be encouraged to talk with a forensic accounting investigator who is trained in working with whistle-blowers. In such an interview, the forensic accounting investigator can form an opinion as to the probable validity of the allegations and can search for the reasons the individual has decided to come forward. The forensic accounting investigator knows there are occasions when people want revenge or attention and use the cover of whistle-blowing to satisfy their own needs. Although all whistle-blowers require immediate and thoughtful attention as required by Sarbanes-Oxley, there should be an attempt to test the allegations for validity—preferably, by face-to-face interview—before the decision is made to launch a full-scale investigation.
- *Discovery that a high-ranking official resigned because of known or possible illegal activities.* Absent evidence indicating an irregularity, a forensic accounting investigator will not usually be called upon to perform an investigation when a high-ranking executive resigns. If evidence of an irregularity does emerge as an issue, the primary initial concern is whether the executive may have acted improperly in other respects. Unless there is a substantial opportunity for financial recoveries, detailed investigation of the known irregularity may not be needed given the executive has resigned. A forensic accounting investigator may perform procedures—including interview and document examination and, very possibly, e-mail searches—to ascertain the likelihood of further improprieties. If it is proved that the executive did in fact knowingly participate in some illegal activities, it may well be the case he has participated in others. Thus, the primary focus of the investigation is on learning the full scope of irregularities that may have occurred. Furthermore, the forensic accounting investigator usually

[5] SMEs refers to professionals who occupy the top rung in the chain of expertise at many public accounting firms. Other terms in this book, such as *forensic accountant,* refer to professionals focused full-time on issues involving fraudulent scheme identification. Such professionals typically work under the direction of an SME whose expertise is forensic accounting investigation.

recommends that the audit team review its audit programs to determine areas in which reliance was placed on the subject executive in the conduct of the audit. The audit committee should be advised that while the investigation is under way, another executive should step in to review relevant prior-year representations so that current-year representations, including Section 302 certifications, are appropriate.

If there is doubt about the integrity of the executive, especially about the CEO or chief financial officer (CFO) who signs the management representation letter, the forensic accounting investigator is likely to search for instances when such executives worked *below* their level of authority and their expected management scope. For example, while interviewing an information technology director, a forensic accounting investigator might learn that the company's CFO was oddly concerned about programming issues and, in fact, would come into the office on Saturdays and do a little programming. Or the CFO had the habit of bypassing accounting supervisors and directly instructing the accounts payable clerk to prepare payments to a certain vendor. Facts such as these—should they emerge—coupled with concerns that the executive has doubtful integrity, could have a substantial effect on the audit program. Early consultation with a forensic accounting investigator may avert problems later, when the company's filing deadline is looming.

- *A client identified as the target of an investigation by a law enforcement agency.* Were the auditor to wait until the investigation is resolved before considering its implications for the audit, that would be a mistake. The length of time to complete an investigation is usually counted in months rather than weeks. In many instances, the company may not even know that the enforcement agency that launched the investigation has concluded it. Consider bringing in a forensic accounting investigator upon first learning of the investigation to discuss its implications.
- *A client who receives a subpoena from a law enforcement or regulatory agency.* A subpoena raises similar concerns as in the preceding scenario. In this case, the forensic accounting investigator usually requests a copy of everything that is turned over to the agency. It would be a mistake to assume that the auditors have previously reviewed all of the subpoenaed documents, even if the auditors specifically requested and did in fact review what they believed to be the full selection of documents. The company may have withheld critical information. For example, the equipment sales contract the auditors reviewed may not have included a key rider allowing the customer to return the equipment under different terms from what was originally provided for in the contract, thereby disqualifying the sale for treatment as a sale under ASC 840 leases. Obtaining another copy at the time of the agency's subpoena gives the auditor and forensic accounting investigator a second bite at the apple. The previously missing rider or other documents may show up.
- *An auditor who believes that intentionally misleading oral information has been provided by the client, or that requested documents have been altered, or that documents are being intentionally withheld.* Auditors may wish to confront the company personnel whom they believe to be involved in the deception. If confronted, an individual may apologize profusely for creating such a

misunderstanding and weave an explanation of some kind around the facts. The audit then continues, but the auditors may be left with the uneasy feeling that they have not received an honest response. Forensic accounting investigators use different techniques. For example, they may make use of indisputable facts about the suspected deception to see whether the individual lies or tells the truth in response to certain strategic questions.

- *Discovery that the client has suffered embezzlement—even of a small amount and even if the suspect is no longer on staff.* SAS 99, paragraph 76, specifically states: "If the auditor believes that misstatements are or may be the result of fraud, but the effect of the misstatements is not material to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the person(s) involved."

  Forensic accounting investigators, honed by years of experience, know that frauds often occur in the most unlikely situations and often are committed by the most unlikely individuals. Any misstatement that suggests the possibility of fraud should be investigated regardless of materiality. The cause may be innocent error. On the other hand, an accounting clerk may have perpetrated a small fraud, or the corporate controller may have a hand in it, and the seemingly small fraud may be only the tip of an iceberg. Suspicions of fraud, regardless of their materiality, require some level of investigation to resolve their implications.
- *Indications that a vendor may be fictitious.* Fictitious *anything* should be a concern. One fictitious vendor may not seem all that important—and it may not be; it may represent a small, unintentional error. But it may also be the footprint of a fraud perpetrated by top management and concealed for years. It is advisable to call in forensic accountant investigators when suspicions about possible fictitious vendors arise—for the simple reason that the range of possibility stretches from an innocent recording error to a very large fraud. If an event does indeed indicate that a fraud may have occurred, both GAAS and SEC regulations have specific requirements as to how to proceed when there is evidence of a suspicious act.
- *Indications that routine transactions have been changed to achieve a different accounting result.* Changes in transactions with no apparent business purpose other than achieving a different accounting result should be a concern and may represent an improper financial reporting scheme. Consider a company that changes the normal method of acquiring a required raw material input at its purchasing subsidiary and selling it to its manufacturing subsidiary. A simple intercompany sale transaction that is eliminated when preparing consolidated financial statements. If changed to insert a third-party intermediary receiving a small commission so that the purchasing subsidiary can record a sale, thereby increasing the top-line performance of the company, the auditor may well be justified in questioning the substance of the transaction and calling in forensic accountants to participate in extended audit procedures—such as interviews with management.
- *Indications of improper accounting for revenue or expenses such as sales recorded before completed and final, goods shipped before a sale is final, revenue recorded while the customer is still owed future service or goods, or apparently false revenues recorded.* The acceleration or outright fabrication of revenue or

the deferral of expenses are among the most common financial statement frauds. While these issues may be investigated by auditors themselves, consultation with forensic accounting investigators may be helpful.

Other indications of fraud that may warrant consultation with a forensic accounting investigator include the following:

- Supplier refunds recorded as revenue
- Unbilled revenues or other accounts receivable being re-aged
- Bill-and-hold issues
- Recording vendor discounts as income
- Revenue recorded from self-dealing or asset exchanges
- Current expenses shifted into later periods
- Expenses improperly capitalized
- Liabilities concealed and not accrued
- Delayed asset write-offs
- Shifting expenses to a later period or advancing revenues

There are a number of other observable events that, while not necessarily indications of fraud, warrant appropriate warnings to the audit staff. The following conditions, either independently or in concert with other conditions, can be red flags of possible fraud. Where all of these conditions are concerned, auditors should proceed with a heightened level of professional skepticism in performing their planned audit procedures. Should indicia of fraud become evident, consultation with a forensic accounting specialist should be considered before proceeding beyond the scope of the audit plan.

Some of the observable events are as follows:

- Transactions that are not recorded in a complete or timely manner or that are recorded improperly as to amount, accounting period, classification, or entity policy
- Managers working below their level of authority
- Unsupported or unauthorized balances or transactions
- Last-minute adjustments that significantly affect financial results
- Evidence of employee access to systems and records inconsistent with the access necessary to perform authorized duties
- Significant unreconciled differences between control accounts and subsidiary records or between physical count and the related account balance that were not investigated and corrected on a timely basis
- Unusual transactions, by virtue of their nature, volume, or complexity, especially if such transactions occurred close to year-end
- Transactions not recorded in accordance with management's general or specific authorization
- Identification of important matters previously undisclosed by management
- Long outstanding accounts receivable balances
- High volumes of sales reimbursements or returns after year-end or both
- Suppliers' accounts with a high volume of debit and credit entries

Conflicting or missing evidential matter may also be a possible red flag suggesting fraud. These conditions include the following:

- Missing documents
- Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist
- Significant unexplained items on reconciliations
- Unusual documentary evidence such as handwritten alterations to documentation or handwritten documentation that is ordinarily electronically printed
- Inconsistent, vague, or implausible responses by management or employees arising from inquiries or analytic procedures
- Unusual discrepancies between the entity's records and confirmation replies
- Missing inventory or physical assets of significant magnitude
- Absence of records relating to the physical existence of inventory such as warehouse receipts, assay reports, transportation or shipping charges, unknown quantities, unspecified quality, or lack of returns or rejections for damaged goods
- Unavailable or missing electronic evidence, inconsistent with the entity's record retention practices or policies
- Inability to produce evidence of key systems development and program change testing and implementation activities for current-year system changes and deployments
- Seriously incomplete or inadequate accounting records
- Transaction structures or contractual arrangements without apparent business purpose
- Unusual transactions with related parties
- Use of agents for no apparent business purpose
- Payments for services that appear excessive in relation to the services provided

Problematic or unusual occurrences between the auditor and the client may also be red flags of possible fraud. Such events include the following:

- Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence may be sought
- Undue time pressures imposed by management to resolve complex or contentious issues
- Complaints by management about the conduct of the audit or management intimidation of audit team members, particularly in connection with auditors' critical assessment of audit evidence or in the resolution of potential disagreements with management
- Unusual delays by the entity in providing requested information
- Tips or complaints to auditors about alleged fraud
- Unwillingness to facilitate auditor access to key electronic files for testing by means of computer-assisted audit techniques
- Denial of access to key information technology operations staff and facilities, including security, operations, and systems development personnel
- Frequent disputes with the current or predecessor auditors on accounting, auditing, or reporting matters

- Unreasonable demands on auditors, such as unreasonable time constraints regarding completion of the audit or issuance of the auditors' report—sometimes accompanied by warnings about the audit fee structure and expected duration
- Formal or informal restrictions on auditors that inappropriately limit access to people or information or that curtail the auditors' ability to communicate effectively with the board of directors or audit committee
- Domineering management behavior in dealing with auditors, especially when there are attempts to influence the scope of auditors' work or the selection or continuance of personnel assigned to or consulted on the audit engagement
- Threats that the working relationship between the company and the auditors will be impaired, perhaps irreparably, if inquiries are pursued
- Client personnel displaying a hostile or unreasonable attitude toward audit personnel
- Client engaging in opinion shopping
- Managers' lying to auditors or evasion in response to audit inquiries to the point that dishonesty seems a likely diagnosis

The ability of auditors to collaborate with forensic accounting investigators varies widely. Some do so comfortably and well, and some do not. Consider this case: An audit manager at a client happens to say to a forensic accounting investigator: "We were doing an audit at a plant in Mexico, and while we were down there, they got an anonymous letter about kickbacks and an outside business interest of the general manager. The client was concerned about costs and didn't want to bring in a forensic accounting investigator, but we were asked to make some inquiries. We didn't turn up anything, so in the end there was nothing to call you about."

Forensic accounting investigators know that many anonymous letters have some degree of merit (see Chapter 8). Even if preliminary inquiries "didn't turn up anything," it might have been safer and been better procedure to presume that something was going on at the plant in Mexico. Failing to bring in a forensic accounting investigation professional to dig deeper, the client now might have had a false sense of security because the auditors had made some inquiries. By letting the client influence their response, the auditors may have served it poorly and also put their own firm at risk.

Would calling in a forensic accounting investigator have cost more? Most likely, yes. If an auditor had been replaced with an experienced forensic accounting investigator, the resulting cost might have been $10,000 more. Is that too much to pay? If the preliminary inquiries uncovered further cause for suspicion, additional investigative procedures might have been necessary—at more cost. But weigh that cost against the magnitude of the direct loss to a company and the damage to reputation resulting from a fraud, especially if the fraud goes undetected for a significant period of time.

Consider the contrast between how a questionable situation might be handled—first without and then with a forensic accounting investigator. The two scenarios are hypothetical, but they run close parallels to plausible events: An accounting firm has audited the financial statements of a client company—a publicly held manufacturer and distributor—since 2000. During that time, the company experienced significant revenue growth while many of its competitors stagnated. In auditing the company's 2007 financial statements, the accounting firm found a large, rounded journal entry

that materially increased revenue. The firm determined that the entry had been recorded manually, while most of the revenue entries were posted electronically from the client's billing system. The manual entry was recorded after the close of the field audit, one day before the company's earnings release.

The auditors questioned the client's controller, who said he had no support for this entry and referred them to the CFO. Both officers had previously worked at the auditing firm and were good friends who socialized with the engagement partner and the senior manager on the account. Questioned about the entry, the CFO said the entry had been made to match revenue with costs in light of entering into a large contract with a new customer after the billing system had been closed. The auditors documented that explanation in their working papers and requested additional support. Later that day, the controller provided a facsimile copy of a customer contract that supported the revenue entry, and he said the original contract had not yet been forwarded from the field to the corporate offices. The auditors documented this in their working papers, along with the facsimile copy of the contract.

Several years later, the chair of the company's audit committee received an anonymous letter that accused the company of fabricating revenue. The audit committee reached out to the audit firm for answers, and the auditors found the following:

- Revenues had been materially overstated each quarter through large, manual, and rounded journal entries entered after the close of the field audit.
- No original supporting documentation for these entries existed.
- The clerk who recorded the entries said the controller had provided on a self-stick note the amounts and accounts to record—with no supporting documentation.

While the auditing firm was looking into these matters, the controller and the CFO resigned. When the board of directors learned of the findings and the resulting restatements that followed, it asked, "Where were the auditors?" The audit firm was eventually fired and later sued in a shareholder class action for malpractice. During the ensuing litigation, it was alleged that the auditors could have uncovered the fraud in its infancy had they investigated the questionable transaction they identified during the 2007 audit. The suit also asserted that the audit firm's investigation had been compromised both by the social relationship between its partners and the corporate officers and by the $1 million-plus fee the firm received from the client for consulting services. Ultimately, the audit firm paid a large sum to settle the lawsuit.

How might forensic accounting investigators have acted in this case? Imagine that after hearing the CFO's explanation of the large, rounded journal entry, the audit firm called in forensic accounting investigators, who suggested that the client's audit committee be notified of the transaction, the lack of documentation to support it, and the CFO's explanation. The audit committee then hired the forensic accounting investigators to investigate, including performing a review of general ledger transactions and the electronic files of the controller and the CFO. The investigative team obtained all general ledger activity from 2005 through 2007 and after consulting with the client's attorney on privacy issues, was able to obtain images of the personal computer files of the controller and CFO.

The forensic accounting investigators found similar large, rounded journal entries recorded late in the closing process for each quarter in 2007, a period when the

industry was contracting. Unlike other journal entries made at corporate headquarters, no documentation was maintained in the central files to support these entries. A spreadsheet schedule on the controller's computer showed that the large, rounded entries matched the difference between system revenues and analysts' expectations. This document was also found to be attached to several e-mail messages between the two corporate officers.

Presented with these findings, the audit committee authorized additional investigative procedures. The forensic accounting investigators interviewed the two officials. The controller said he had been pressured by the CFO to record these entries and acknowledged that they were inappropriate. The CFO stood by his previous explanation and denied wrongdoing. Both men were placed on temporary leave and escorted from the building.

Subsequent interviews with employees of the accounting and finance departments produced invoices for payments made to certain vendors that had been authorized by the CFO. The forensic accounting investigators examined the company's vendor master file and found more than ten vendors with the same post office box number. A review of the canceled checks to these vendors found that all of the checks had been deposited into the same bank account and that they totaled more than $1 million.

The audit committee notified the authorities and its insurer. An investigation led to criminal charges against the two officers. The successful investigation cemented the audit firm's relationship with the client.

RELIANCE ON OTHERS

When concerns arise that require a company to undertake a 10A investigation, consider the possible advantages of early involvement in working with the company's audit committee and its 10A counsel to determine the possible financial statement impact.[6] While it is true that it is the company's responsibility to conduct the investigation, early involvement on the part of the auditor could be advantageous to the company's goals of resolving the allegations and concerns so that regulatory filings can be timely made and the company can get back to normal operations. Also, to fulfill their own 10A responsibilities, auditors may consider calling upon forensic accounting investigators to advise on the conduct of the investigation and whether

[6] A 10A investigation refers to an outside investigation, that is, one conducted by individuals independent of management or the board of directors; from Section 10A, "Audit Requirements," of the Securities Exchange Act of 1934 [Public Law 73-291, 73rd Cong., 2d sess., 13 (1934), sess. (January 23, 2002)] as amended by Section 301—"Public Company Audit Committees" of the Sarbanes-Oxley Act of 2002 [Public Law 107-204, 107th Cong., 2d sess. (January 23, 2002)]. "Section 10A of the Securities Exchange Act of 1934 (15 U.S.C. 78f) is amended by adding at the end the following:
(m) Standards Relating to Audit Committees—
. . . (5) Authority to Engage Advisers
Each audit committee shall have the authority to engage independent counsel and other advisers, as it determines necessary to carry out its duties. . . . "

or not its scope and procedures are adequate for the auditor's needs. This is usually done by shadowing the lawyers and forensic accounting investigators engaged by the audit committee. The practice of shadowing can provide greater comfort that there will be no surprises at the conclusion of the company's investigation.

In one such investigation, forensic accounting investigators received a call from an auditor, informing them of a recently concluded 10A investigation on one of his audit clients. The 10-K was due to be filed the following week. The auditor disclosed the nature of the investigation to forensic accounting investigators from his own firm. The investigation had been conducted by outside counsel, who had been retained by the audit committee. Outside counsel had chosen to conduct the entire investigation without the use of forensic accounting investigators. As the auditor recounted the allegations and the procedures performed by the law firm, the forensic accounting investigators on the call knew instantly that there were gaping holes in the investigation. The allegation was that the CFO had instructed divisional controllers to create false entries that inflated revenues. The CFO had contended in an interview that it was all a misunderstanding and that the error was already corrected. First of all, was an e-mail review performed? Yes. However, the law firm had accumulated the e-mail data by requesting the company's information technology department manager to "copy" e-mail folders. Experienced forensic accounting investigators know consideration should be given to collecting e-mail on servers and hard drives through forensic imaging, thereby capturing all deleted files. Merely copying the drives will not capture deleted files. Second, the law firm performed no assessment of the likelihood of involvement in the alleged scheme by anyone in the information technology department. The forensic accounting investigators told the auditor that because of these and other deficiencies in the conduct of the investigation, he should not rely on its results. "Then what am I to do?" asked the auditor. The forensic accounting investigators suggested he contact his risk management group within the firm for further consultation on the various options to consider for possible resolution of the potential issues.

With proper planning, problems such as these may be avoided. The audit firm's own forensic accounting investigators can be called in under the scope of the existing audit engagement letter and set to work immediately. While it is certainly true that conducting an investigation into possible illegal acts is the responsibility of the audit committee, the auditor also has to be satisfied that the investigation is conducted in an appropriate way by competent people who know the requirements of 10A.

CONCLUSION

The decision as to whether to bring in forensic accounting investigators is a judgment call. There is certainly no requirement in the professional standards of GAAS to do so. The benefits of consulting with forensic accounting investigators have been evaluated since the passage of Sarbanes-Oxley and are better appreciated by auditing firms as well as the companies that use their services. If you were to ask investors and other stakeholders, they would be likely to say, "The more accountants sniffing around, the better." But even forensic accounting investigators would tell you this is not necessarily true. The profession should strike a balance between auditing to obtain

"reasonable assurance" that the financial statements are free of material error and doing so in a cost-effective manner. It makes little sense to impose a tremendous cost burden on society to pay for fraud audits at every company. Since most companies' managements consist of honest people working for the good of the company and its stakeholders while complying with laws and regulations, conducting overly extensive and invasive audits does not make sound business sense. Yet the more that can be done to reduce the likelihood that a material fraud will occur and go undetected by the company, its auditors, or its regulators, the better.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 6

Internal Audit: The Second Line of Defense

Dennis D. Bartolucci, Therese M. Bobek, and James A. LaTorre

Our chapter title is a deliberate provocation: If internal auditors are only the second line of defense against the occurrence of fraud in an organization, what is the first line of defense? The answer is clear: management. Management is preeminently responsible for fraud deterrence in two respects. First, through the example it sets—the tone at the top—management is first to deter and defend against corporate wrongdoing of all kinds. The ethical tone of the entire organization depends to a significant degree on how top management is perceived both day to day and in its handling of crises. And second, management is responsible for the system of internal controls that should be implemented throughout the entire organization to control, monitor, and document higher-risk areas such as revenue recognition, cash management, purchasing, and inventory.

Management must base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts. As outlined in detail in Chapter 1, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published *Internal Control—Integrated Framework,* which has emerged as the framework that management and auditors use to evaluate internal controls. The five components of the COSO internal control framework are the following:

1. The control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring[1]

Although antifraud programs and controls must include all five components of the COSO framework, special emphasis is placed on the control environment: the tone set at the top of an organization that influences the control consciousness of

[1] PricewaterhouseCoopers, *Key Elements of Antifraud Programs and Controls: A White Paper* (2003), 26–27.

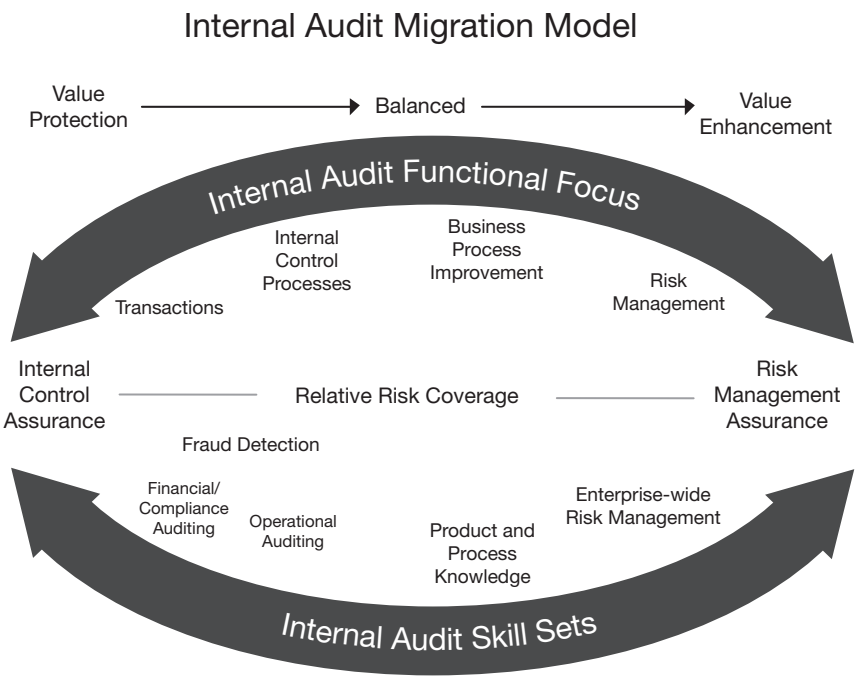


EXHIBIT 6.1 The *Football:* Internal Audit Migration Model

its people. This environment includes management accountability and oversight of antifraud programs and controls. Since 90 percent of all financial statement fraud involves senior executives, the establishment of strong antifraud programs and controls is an essential component of a healthy control environment.[2]

This said, there can be no doubt that the internal audit unit of a company is, indeed, the second line of defense.

WHAT DO INTERNAL AUDITORS DO?

The common misunderstanding is that internal auditors do what external, independent auditors do but they do it earlier—that is, they focus on financial accounts, financial accounting systems, and financial risk controls so that the house is in good order when the external auditors arrive. This is a partial truth. In reality, the internal audit function can be remarkably diverse. While some internal audit units do focus predominantly on financial accounting and the financial control environment, others have much more elaborate agendas requiring a broad mix of skills and experience.

Such a diversity of missions and skills is captured in a chart we informally call the *football* (Exhibit 6.1). Reading from left to right, the chart identifies at the left the traditional missions and skill sets of the internal audit function. Progressively to

[2] Id., 3.

the right are more diverse and more sophisticated functions, matched to skill sets, which have become the mission of internal auditors in companies and industries that expect more from their internal auditors. The range, then, is from a strict focus on financial auditing, dedicated very largely to value protection, to an elaborate role as a multiskilled consulting entity within the organization, dedicated to value enhancement. No place on the football—no particular mix of tasks and skills—is better than any other. What matters is the alignment of the internal audit unit with the level and type of risk monitoring that management and the board view as internal audit's mission. Because that view is almost sure to change over time in response to a company's needs and to regulatory requirements, the spot the unit falls on the continuum will also change over time.

In a company that chooses not to make aggressive use of the internal audit function but that nonetheless looks to it for specific and critically important services, internal auditors are likely to be responsible for the first three functions named in the upper arc of the chart:

1. Transaction auditing
2. Internal controls evaluation
3. Business process improvement

Internal auditors examine accounts and transactions together with the underlying infrastructure of accounting systems and built-in risk controls. To clear up discrepancies or clarify the exact nature of a problem, they will "ask the next question"—an action of real importance to their work—of those responsible for the accounts and systems. If they identify a control deficiency, they recommend to management certain appropriate solutions. With respect to business processes, they're constantly on the lookout for inefficiencies and better ways to work, again making recommendations to management. Such process reviews and recommendations as to best operational practices may and should make a huge cumulative difference in productivity, profitability, and employee morale—this last in the sense that most people prefer to do things as efficiently and effectively as possible.

Further to the right around the arcs in Exhibit 6.1, the internal audit function becomes an increasingly diverse consulting unit, expert in many types of risk and the management of those risks and charged with the holistic mission of enterprise risk management. The model for internal auditing at this level of sophistication is often thought to be that of the General Electric Company (GE), whose internal auditors have historically been business process reengineers, best-practice implementers, and cost cutters. Out of some 300 to 400 internal auditors at GE, many have MBAs, and a third or more are Six Sigma trained. While the left side of the chart indicates that they remain responsible for traditional internal audit skills and services such as financial auditing, they cover the full spectrum from left to right. To address GE's diverse businesses, the company's internal audit group includes financial auditors with specialized knowledge of the plastics industry, the chemicals industry, life sciences, and other fields.

Returning to the left side of Exhibit 6.1, you will notice that *fraud detection* is positioned among the traditional, financially focused internal audit missions. This both is and is not an innovation—and the ambiguity bears discussion. *Fraud deterrence* has always been a function of internal auditors. The periodic presence of

capable internal auditors visibly at work in geographically separated business units or at headquarters is in and of itself a deterrent. *Fraud detection* also represents a traditional task of the internal auditor, but recognition of the need for fraud detection has vastly increased in the last decade. The internal audit function is often well placed to offer this service—provided that members of the team have acquired training in fraud detection, which encompasses everything from attitudes and methods to knowing when the red flags of possible fraud are vivid enough to call in forensic accounting specialists. Responding to the increased emphasis on fraud detection, internal auditors are—and should be—seeking the specialized training that truly makes them the second line of defense after management. In fulfilling their mission in the area of fraud detection, they function much like external auditors. And like external auditors, they need to be clear about the dividing line between the audit role and a forensic investigation. (See later in this chapter and also Chapter 3.)

Movement from left to right within Exhibit 6.1 does not mean that the basic missions of the internal audit function get deemphasized as more sophisticated agendas get added. The movement is accretive, adding skills and functions while retaining the fundamental focus on transactions and controls. However, the percentage of time allocated to one function or another along the continuum varies according to the priorities of management and the board.

INTERNAL AUDIT SCOPE OF SERVICES

Management and the board set the scope of internal audit services, typically on an annual basis. In most companies, the director of internal auditing still reports administratively to the chief financial officer (CFO) or controller, who controls the budget and periodically reviews the activities of the function. Functionally, however, in the post–Sarbanes-Oxley Act of 2002 environment, in many companies, the internal audit staff reports to the audit committee. (Later in this chapter is a discussion of the impact of reporting relationships on the internal audit.)

Through the decade or so before the collapse of Enron and other major firms amid allegations of massive fraud, the agenda of many internal audit groups tended to move toward the right in Exhibit 6.1. Internal auditors were increasingly asked to function as multiskilled risk consultants, thus allocating a larger share of their budget to consulting tasks than to the narrower set of functions named at the left of the chart. For the most part, this has now changed, owing primarily to two factors. In the first place, during difficult economic times, companies are less willing to field a multiskilled, high-cost internal audit team to address enterprise risk management in the style of consultants. Under those conditions, companies tend to refocus on value protection, reduce internal audit budgets, and put the emphasis on financial and operational efficiency auditing. Internal audit is a cost center, not a profit center; as such, it is susceptible to budget cuts during economic downswings and sometimes has to fight for its fair share against competing management priorities.

Second, as we just implied earlier, the catastrophic accounting frauds at major U.S. companies and the stringent new legislation and regulation to which they gave rise have forcibly turned the attention of management and boards toward the need to ensure the integrity of financial accounting and reporting. This, too, has swung

the pendulum back to the left, toward the basics of internal auditing and with greater emphasis on fraud detection.

The pendulum will continue to swing, responding not only to large-scale external circumstances such as the economy, major business events, and regulatory change but also to internally recognized needs. For example, if a company whose internal audit unit is focused on enterprise risk management makes a large acquisition, internal audit may well resume the traditional focus on finance and operational efficiency. An internal audit group focused on internal controls and process improvement can tell management a great deal about the operations of a new acquisition and then make scores of useful recommendations. Similarly, as companies expand around the globe, management is likely to rely on the internal audit function to provide assurance concerning the integrity and appropriateness of financial accounting and controls in geographically separated units.

There is another issue of scope that influences the fraud detection capability of internal audit units. In their business lives, some people who do not typically interact with internal auditors often believe that internal auditors visit all parts of even the largest enterprise at least annually—that they act as the cop on the beat, never far from the neighborhood. However, in large, geographically decentralized organizations, this is rarely true. The annual risk assessment and definition of the internal audit agenda—for which senior finance executives and the directors of internal audit units are typically responsible, subject to audit committee review—determine which units of a company are to be audited in that particular year. The issue is quantifiable: "We have 40,000 hours of internal audit time to spend this year. Where should we spend them?" If the external auditors are known to be emphasizing contracts in a given year, the CFO may decide not to focus the attention of internal auditors in that area, because the time may be better spent elsewhere. Similarly, the CFO may schedule visits to business units in which there is either a suspicion of difficulty or likely opportunities for operational improvement. At any given unit, several years may pass between one internal audit visit and the next. This illustrates all the more clearly that management, which institutes the controls embedded in financial systems and business processes and which owns those controls on a day-to-day basis, is the first line of defense in deterring fraud.

THE HANDOFF TO FORENSIC ACCOUNTING INVESTIGATORS AND LEGAL COUNSEL

Internal auditors operate in a network with other key players: management, the board, external auditors, forensic accounting investigators, legal counsel, and security personnel of various kinds. For purposes of fraud detection and the proper conduct of a fraud investigation, knowledgeable cooperation among internal auditors, forensic accounting investigators, and in-house legal counsel is essential. While cooperation with information technology security managers and (in industries such as retail) loss prevention specialists is also critical to a company's welfare, the renewed emphasis on fraud detection as a role for internal auditors puts the spotlight on how internal auditors interact with forensic and legal investigators.

When should internal auditors alert management and legal counsel that a fraud is suspected and call in forensic accounting investigators to investigate? The answer

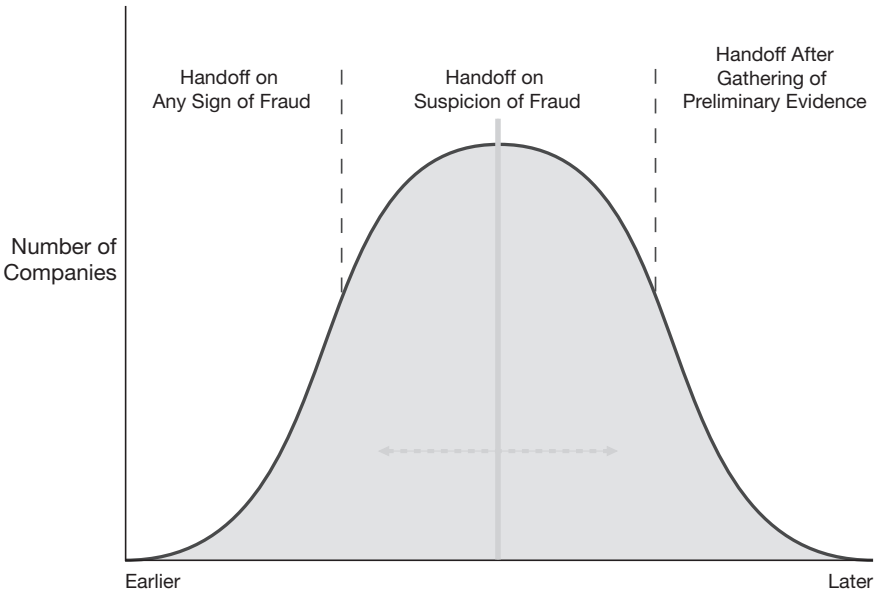


EXHIBIT 6.2 Timing of Handoff to Forensic Accounting Investigators

depends on many factors: management's policy, the skill sets and experience of the internal audit team, legal counsel's policy, and the emerging set of best practices to which this book is a contribution. These factors interact to create, in effect, a bell-curve chart.

In Exhibit 6.2, the far left shows companies whose management considers that any sign of fraud should be considered the tip of an iceberg until proved otherwise; therefore, forensic accounting investigators and legal counsel are brought into the picture at the earliest stage. In the midsection of the bell curve fall companies—arguably, a growing majority—that require internal audit to call in forensic accounting investigators as soon as a suspicion of fraud has been detected. Because it knows the company best, the internal audit team is likely to contribute members to the forensic accounting team that sets to work, but responsibility for the investigation rests with the forensic accounting investigators. At the far right in Exhibit 6.2 are companies that authorize their internal audit units to independently gather preliminary evidence concerning a possible fraud. When they uncover evidence indicating that forensic investigation and preservation of the chain of custody over information would be prudent, they refer the matter forward.

There is, or should be, a bright yellow line separating deterrence and detection from investigation. Internal auditors need to continually improve their abilities to uncover indicia of fraud. Internal audit should be fully capable of probing the scope and character of a suspicious situation—yet also willing, if not required, by policy to bring in forensic accounting investigators and legal advisors when suspicions arise. Some internal auditors may say that until they're certain of the fraud, they should investigate a suspicion of fraud and not bring in forensic accounting investigators. This can be a mistake. The advantage of calling on forensic accounting investigators at the first suspicion of fraud is that such investigators are trained in the art of

determining the next steps: the specific investigative procedures required to determine whether a suspicious circumstance is, in fact, a defalcation.

The investigation begins when routine audit procedures end. Any other deployment strategy runs a high risk of missing the fraud during the sniffing-around period that follows a suspicion of fraud and precedes the discovery of a defalcation. No matter what the internal auditors' level of training or certification—such as certified fraud examiner (CFE)—the moment comes when they must say, "At this point, we're handing it off to forensic accounting investigation professionals."

PERCEPTION PROBLEM

Generally speaking, internal auditors have invested much time and care into building cooperative relationships with other company personnel. In the early days of internal auditing, their reputation within companies often had some of the flavor of their being internal police—the inspectors who are determined to find fault and discomfit the executives and staff of audited units. Internal auditors soon enough understood that that reputation tended to cut them off from the very people—managers, staff at all levels—with whom they had to interact in order to understand the quality of internal controls and to uncover opportunities for greater operational efficiency. Accordingly, they learned to emphasize the positive impact of internal audit inquiries, tests, and recommendations: "We're here to help you, not hurt you." Also, in companies whose internal auditors function as a multiskilled consulting unit with a value enhancement agenda (the right side of Exhibit 6.1), those internal auditors enjoy considerable prestige.

Given this background, the stronger emphasis on fraud detection must be handled with sensitivity. On one hand, internal auditors do not wish to turn back the clock to the early days of fear and wariness. On the other hand, they cannot and should not disguise their mandate from management and the audit committee to dive deeper, to look for suspicious signs, and to deter and detect fraud. Now, more than ever, communication often constitutes 50 to 70 percent of an internal audit. If internal auditors cannot gather information from managers and staff in an atmosphere of collegial cooperation, their work is severely hampered. Value-added recommendations about improving controls or business processes depend in good measure on information freely offered. Internal auditors can look at huge amounts of data—and they certainly do that—but it is likely to be much more difficult to validate findings in the data and understand the implications of those findings unless managers and staff help out willingly.

We refer repeatedly in this book to the point of transition—the point at which auditors (internal or external) should consider calling in forensic accounting investigators to address a possible fraud. Because over the long term they must preserve cooperative relations with the vast majority of managers and staff in their company, internal auditors have good reason to call in forensic accounting investigators once they've uncovered a suspicion that a fraud may exist—beyond their original risk assessments. The forensic accounting investigation is likely to be conducted discreetly during its earlier stages, but ultimately, it may give rise to forceful, disturbing events. The internal audit team may assist with the investigation, but it is in their interest for the forensic team to lead the investigative effort and shape whatever communications about the outcome must eventually be disseminated within the unit or the company.

Statement on Auditing Standards (SAS) No. 99 instructs external auditors to take a neutral attitude with respect to management's integrity and to exercise professional skepticism in the conduct of their procedures. Also, the standard instructs the auditor to assume that a risk of fraud does in fact exist. Both of these provisions are counter to many of the internal auditor's objectives. It is mission critical for internal auditors to gain the trust and confidence of those with whom they work. They are virtually certain to have developed close working relationships with the very people who may have committed a fraud. For this reason, they are not well placed to conduct a formal fraud investigation, and the appearance if not the reality of a lack of objectivity toward company personnel could be viewed as a departure from the Standards of Professional Conduct of the Association of Certified Fraud Examiners.

COMPLEX CORPORATE FRAUD AND THE INTERNAL AUDIT

The continuing wave of high-profile, complex frauds involving billions of dollars, wayward accounting, and catastrophic corporate failures raises many questions, including this one: Where are the auditors? The question could be asked about both the external *and* the internal auditors.

Two common reasons that have surfaced in cases for failure to discover fraud are:

1. Deference to senior management regarding complex financial transactions and instruments
2. Limitations on the information and scope that are being provided for internal auditors

WORLDCOM AND THE THORNBURGH REPORT

The bankruptcy proceeding in the aftermath of the exposure of WorldCom's monumental accounting misdeeds included a document known as the Thornburgh Report, which highlights several potential considerations, pitfalls, and lessons learned that internal auditors may confront in the course of their work.[3] Another document of interest is the report issued by the special investigative committee of the board of directors of WorldCom.[4] In what follows, we draw first from the Thornburgh Report:

- Maintain increased skepticism; this may contribute to discovering potential red flags of fraud in earlier periods.

[3] Dick Thornburgh, Bankruptcy Court Examiner, First Interim Report of Dick Thornburgh, Bankruptcy Court Examiner, United States Bankruptcy Court, Southern District of New York. In re: WorldCom, Inc., *et al.*, Debtors. Chapter 11, Case No. 02-15533 (AJG) Jointly Administered, November 4, 2002.

[4] Dennis R. Beresford, Nicholas deB. Katzenbach, and C. B. Rogers Jr., Report of Investigation by the Special Investigative Committee of the Board of Directors of WorldCom, Inc., March 31, 2003, http://news.findlaw.com/hdocs/docs/worldcom/bdspcomm60903 rpt.pdf.

- Be wary of certain limitations that may hinder internal auditors' abilities, such as management's direction to focus on operational issues rather than financial matters.
- Real support from senior management, the board, and the audit committee[5] is crucial to being effective.
- Evaluate the actual financial statement fraud risk, especially in organizations that may have an increased risk "due to the complexity and dispersed nature of the company's organization and financial operations."[6]
- Strive for adequate annual internal audit planning if the annual plan is not followed, and determine whether this is the appropriate course of action.
- Strive for actual and active contact with the audit committee rather than relying on others. A warning may be observed from the Thornburgh Report: "There is no evidence that the Audit Committee requested from the Internal Audit Department updates on the status of internal control weaknesses."[7]

The report of the special investigative committee adds a further insight and potential lessons:

- Strive for open communication between employees and the internal audit personnel.[8]
- Focus on substantive interaction between the internal audit personnel and the external auditor.

Courage may be required to continue to probe in certain areas, especially in an environment that is not transparent or when facing objections from management. Open communication with the audit committee as well as external auditors and advisors may be able to offer assistance to internal auditors when faced with these situations.

With proper training, knowledge, and experience, internal audit can have a central role in directing the compass for fraud detection. Qualities such as professional skepticism and personal courage may be needed to establish the truth. However, in some environments, it is also possible that internal audit can be deflected from its primary mission: the auditing of what its risk assessment indicates are key areas requiring audit. What should have been an essentially routine activity took extraordinary courage to accomplish.

CASE STUDIES: THE INTERNAL AUDITOR ADDRESSES FRAUD

The following brief case studies are varied examples of fraud and its detection, ranging from complex fraud by a master fraudster to many types of common fraud that

[5] Thornburgh, First Interim Report, chap. V, § E-3, "The Company's Internal Audit Function," 52.
[6] Id., 55.
[7] Id., 56.
[8] Beresford, *et al.*, Report of Investigation, 18.

can create, over time, a damaging drain on company assets. Perhaps more effectively than any theoretical explanation, these cases demonstrate the value of professional skepticism, the almost-sixth-sense awareness that arouses the suspicion of an able internal auditor, and the cooperation that is needed with upper management, forensic accounting investigators, and others to expose and eliminate the more serious types of fraud. Several of the cases also demonstrate the real-world constraints within which internal auditors must sometimes operate. The following mottoes, which we propose as a preface to these cases, represent the folk wisdom of two senior internal auditors who contributed several of the cases:

- Liars can figure, and figures can lie
- Every good internal auditor is from Missouri, the Show-Me state

No Segregation of Duties—and a Very Nice Car

While visiting an outlying plant in the American Southwest, a finance executive from headquarters made a mental note when he saw that an accounts payable supervisor (the AP) was driving a Seven Series BMW—quite a car for an individual earning something on the order of $60,000 annually. Asked to respond to this potential red flag, the internal audit unit observed that segregation of duties had not been properly built into the accounts payable system, so that the AP was able to manipulate all parts of the system. Also, a certain number of checks—how many was not yet clear—were being mailed to post office boxes rather than to normal vendor addresses. These preliminary indications of fraud were reason enough to call in a forensic accounting team.

Working with the internal auditors, the investigating team soon discovered that the AP had created fictitious vendors and routinely cut checks to them. The checks were showing up in private mailboxes, from which he would harvest them periodically. The team downloaded data on vendors in the preceding 24 months and discovered that fully 90 percent of them were fictitious. In that 24-month period, the AP had misappropriated $600,000.

The division of labor between the internal audit group and the forensic accounting experts was classic. The internal auditors were able to pull the financial picture together without alerting the target individual, while the forensic team did a full financial check on him: house, cars, and much more. The forensic team also interrogated data extracted from servers and hard drives and used this information to build a case. Convinced of the AP's culpability, the forensic team conducted the admission-seeking interview, which, on the basis of overwhelming evidence, achieved its purpose. A report to the company's audit committee was drawn up jointly by the leaders of the two teams at the conclusion of the effort.

Case closed? Not yet—the internal audit team had further work not just at the plant but also across the company. The company's enterprise-wide financial system was compatible with a software tool that enabled the team to run a segregation-of-duties test for everyone in the company. Did any employees have access levels that were incompatible with their duties? If an employee did have incompatible access rights, was there a valid reason? Were mitigating controls in place? On the basis of this analysis, internal audit went on to redesign the pattern of authorities and

accountabilities, and it closed many loopholes, including the one through which the dishonest AP had driven his fraud.

Odd Transportation System

A company with several new plant locations was spending $3 million a year on van service to transport employees from one plant to another and back again. From an external audit point of view, there were only a few questions to ask about this arrangement: "You say it's a $3-million service? Fine. Vouch that amount and make sure that you have $3 million accounted for, with checks written to the van lines." There is no operational question or critique in the external auditor's approach. On the other hand, the internal auditor thinks differently. "Hmm, you're using ten van lines. What if we narrow it down to two van lines and insist that they compete—promise them bulk business if they offer better rates. We could easily save $2 million."

Brilliant! But in actual fact, the internal auditor still is not exercising enough professional skepticism and should ask the next question: "Why, in the first place, were there ten van lines, when anyone could see that two competing lines would make better business sense, and did someone's brother-in-law own one of those van lines?" Probably not—probably the whole arrangement just grew without critical oversight, but questions of that type need to be kept in mind. The new mind-set of the internal auditor is to be ceaselessly aware of the possibility of fraud. The new agenda should be to dive more deeply than in the past. It may cost more to investigate in depth some minor common fraud than to close it off and move on, but it is always worthwhile to ask the next question.

A TRAGIC CIRCUMSTANCE

Recall from earlier chapters that corporate fraud occurs—if it is going to occur at all—when the three factors of the fraud triangle coincide: need, opportunity, and rationalization. This case represents a tragic example of the compelling factor of need.

The internal audit team was executing a routine match of employee payroll records to benefits enrollment lists as a way of checking whether the benefits administration was deleting terminated employees in a timely manner from enrollment in the benefits plan. If there was any lag, the company would be losing a few hundred dollars per month. The team identified an individual enrolled in the plan whose name did not match any employee records. Naturally, they went to the benefits administrator, an older woman long with the company, to inquire. "That person doesn't work here," she said.

Something in her attitude and in the facts themselves prompted the internal audit team to dig deeper. As there was clearly a suspicion of fraud, forensic accounting investigators were brought into the engagement. Here is what they discovered—initially, through discussion with the controller, and later, through an investigation conducted by the forensic accounting team. The nonemployee enrolled in the plan was in fact the administrator's son. In the timeframe under review, he was 22, had been suffering from cancer and needed extensive treatment, and had no medical coverage of his own. With no one to turn to, the administrator had signed

him up as a member of the self-insured plan. Some months earlier, he had passed away, and the company had incurred $150,000 of self-insured medical expenses before his death.

How could the administrator bend the system to her purpose? Because she was trusted and well-known to the insurance company's own administrators, she had called them up, explained that she had forgotten to enroll an employee, and asked them to backdate his enrollment to the beginning of the year. Having no reason to doubt her word, the insurance company's people complied with her request and sent the enrollment forms and all change notifications directly to her. Information about the plan enrollment would go periodically to corporate headquarters, where no one knew Bill from Steve from Harry, and so no one was the wiser.

In this case, a routine check to save the company unnecessary expense led to a tragic instance of fraud. The company terminated the administrator but under the circumstances took no further action.

How Many Lunches Can You Buy?

Not every fraud is theft for personal benefit. Some fall into a gray zone of clearly unethical conduct but no greed or malice. An internal audit team was conducting a routine review of petty cash accounts. The average balance was $800, as expected, but the volume of money going through these accounts was $8,000 to $10,000 a month. Why? The team looked more closely. The company had imposed a strict limit on capital spending that year: "Times are tough." "Cut your capital budget." "Don't spend." But this particular unit of the company had a towering need for new computer equipment. With the capital appropriation request process basically at a standstill, the unit's information technology people had decided to buy computers and related items such as office furniture by using petty cash. They did not report the acquisitions, and they kept the petty cash accounts at about the right level at any point in time.

It was not a dramatic fraud, but it was certainly a circumvention of policies. The managers further up, who understood why capital spending had to be curtailed, were not pleased to learn about this concealed activity at the unit. From the internal auditors' perspective, the key thing was to notice the potential red flag. How many lunches can you buy?

Forensic accounting investigators were called in to review the work of the internal auditors, who had uncovered the fraud rather quickly through only one procedure. The forensic accounting investigators knew how to search for other indications of fraud by way of ensuring that the fraud was confined to this small group and only this scheme.

Making the Numbers Look Right

An internal audit team at a major company was carrying out inventory audit procedures. One of the standard tests is to look at the reconciliation between booked inventory and actual physical inventory, which naturally requires the team to go out on the floor to quantify inventory on hand and then compare that measure with inventory recognized in the system. The team started on this laborious process and quickly came up with differences that nobody was able to explain. Looking more

deeply into the total reconciliation process, the team realized that nothing made sense. It was time to talk with the controller, who was responsible for inventory accounting.

The internal audit team leader had hardly begun the discussion, when the controller became tremendously upset and offered what amounted to a confession, as if this purely exploratory meeting were an admission-seeking interview. The auditor accepted the circumstance and listened carefully. The controller said he had been hiding variances by means of multiple journal entries in balance sheet accounts, thereby moving the numbers around to come up with an inventory that actually seemed to be accurate.

After he started trying to make the numbers look right, he said, he found himself caught in his own game and continued to hide one erroneous entry with another—until the whole process had spiraled out of control.

The internal auditors called on inventory experts from elsewhere in their organization to untangle the mess the controller had created. Meanwhile, a forensic team probed the accounts and the surrounding circumstances—including the individual's lifestyle and financial condition—to ascertain whether a defalcation had actually occurred. Nothing remarkable was found. The scheme proved to be a matter of abysmally bad judgment, unrelated to any personal gain other than making the numbers look right in the eyes of upper management. The individual was fired, and the damage he caused was kept within bounds.

It was entirely appropriate for the internal audit leader to meet with the controller to inquire about the reconciliation. Before this meeting, all he had was a number of questions to better understand the reconciliation process; there had been no indicia of fraud. In that meeting, the controller voluntarily confessed and the internal audit leader realized he would want to bring in forensic accounting investigators to clarify matters, but meanwhile, he was in the middle of hearing a confession. He did the right thing by continuing the interview. It would have been foolish on his part to say something like, "Can you hold that thought until I can conference in a forensic accounting investigator?"

There might not have been a second chance; now was the time to listen. When the perpetrator of a scheme decides to confess, take notes, be consoling and appreciative, and get through it as best as you can. You can call on the forensic accounting investigator later, who is likely to arrange another interview.

How Not to Earn a Bonus

Fraud is sometimes the bad result of a problem that could have been solved by better management. An internal audit team was performing a normal test of inventory at a major facility in the tourism industry when it discovered two to three times as much inventory on the balance sheet as could actually be found in inventory. The inventory balance had grown to approximately $1.2 billion, while the physical, at-hand quantity on the books was on the order of $500,000. They knew this was not right and persistently asked the next question.

Soon they discovered a rather complicated scenario involving greed and pressure tactics. It turned out that the head of food and beverage, an extremely aggressive individual, had been pressuring the controller to keep cost of sales no higher than a certain level. He had managed to convince the controller that the fairly high cost of

sales was an accounts payable problem—that the accounts payable unit had double paid and triple paid invoices in some cases, thereby causing the cost of sales to appear higher than it actually was and throwing off the inventory balance. Caving in to the pressure and the spurious argument, the controller transferred the entire excess inventory into a prepaid account to hide it. This was done literally at 11 P.M. on the night before the books were to close for the year.

When the internal auditors sought out the controller to shed light on the inventory problem, he stalled them: "We'll investigate next month." That was not a good enough answer. The head of internal audit informed senior management of the problem, and his group pressed forward with an investigation, conducted by forensic accounting investigators. Soon things began falling into place. The bonus of the food and beverage director had been dependent that year on keeping cost of sales below a certain level.

The situation was corrected in cooperation with management and the external auditor. On one hand, an inventory write-down had caused the company to fall short of its revenue goals for awarding bonuses that year. On the other hand, the head of internal audit had been awarded a handsome bonus for detecting the potential red flag and courageously reporting up the line to senior management—for all he knew, at the risk of his own bonus. The food and beverage director, the controller, and several others were terminated.

In the course of the investigation, a curious fact came to light: an accounting supervisor in the food and beverage area had been aware of the manipulations, knew they were wrong, and had been trying to get people's attention. In response to his efforts, he had heard nothing but "It will be taken care of." True, he could have tried harder. For example, he could have spoken with the internal auditors. But he had nonetheless demonstrated integrity, judgment, and a measure of courage. He was promoted to the position of food and beverage controller. The company also installed a hotline facility and began an education program throughout the company so as to avoid any future problems regarding employee attempts to communicate suspicions of fraud.

In the months following the inventory write-down and dismissals, some relatively straightforward and wholly legitimate business and accounting changes were made, and the cost-of-sales problem was solved. Had the food and beverage director managed more effectively, he would have been able to drive the cost of sales down to his bonus target through legitimate means.

A Classic Purchasing Fraud

The distinction between common fraud and complex fraud is worth keeping in mind. The internal auditor is charged with making a best effort to detect both. One of the most common types of fraud is illustrated in this case. Though common, it can cause considerable harm if it goes undetected.

An internal audit team was performing a review of a company's payables department. As part of that activity, the team was performing routine tests on a sample of purchases to verify whether they had been properly authorized. In the sample there was a vendor called United Tech—a name very like United Technologies, a major enterprise from which the company actually did make purchases. The auditors felt uneasy about the abbreviated account name. Why would this vendor

name track so closely with the name of a major company? They decided to look more closely.

Suspicious signs soon turned up. The paid-to address of United Tech was a post office box, and other features of the vendor records seemed atypical. The audit director talked the matter through with the CFO at that business unit, who agreed there was reason for suspicion. More digging disclosed that United Tech was not, in fact, a legitimate vendor. With the help of a forensic accounting team, it was time to piece together the nature of the fraud.

Here are the facts that emerged. A former employee in the information technology department of the company who had access to all of its software had recorded that vendor in the company's master file. Circumventing all normal procedures, he then created transactions in the name of United Tech.

In reality, United Tech was not a legitimate business but an offsite mailbox to which company checks for fictitious goods and services were delivered. The fraudster would stop by from time to time to gather up his latest haul of checks.

Once these facts of mail fraud had been established, management called in the U.S. Federal Bureau of Investigation, which staked out the mailbox and observed the former employee picking up his mail. A strange feature of the case—and a useful warning to internal auditors and forensic accounting investigators—is that this individual was able to continue the fraud for six months after leaving the company because he continued to have access, from a remote location, to the company's computer systems.

This individual was prosecuted and served jail time.

The Loneliness of the Internal Auditor

This case, concerning domestic pressures to overlook fraud, relates closely to the preceding international case. An internal audit team and, ultimately, the internal audit director became aware that the sales manager of a business unit was defrauding the company through his expense reporting. This fellow did not have much talent for fraud: Using tear-off restaurant tabs to submit charges as though they were business meals, he overlooked the fact that the tabs were consecutively numbered. His expense reports showed food expenses sequentially numbered—13101, 13102, and so on—from report to report. This potential red flag had shown up in a routine audit of expense reporting in his department. It was obvious that he was cheating on his expense report, and forensic accounting investigators soon discovered that in his private life, he was buying gifts in the range of $75 to $200, roughly the price of meals with customers. He had converted his expense report into a small but reliable cash cow.

That is the dull part of the story. The interesting part of the story is that the sales manager's brother was a powerful executive in the company. When this issue came to light, something happened behind the scenes along the lines of a heart-to-heart conversation between the controller, to whom internal audit reported, and the influential brother. The words of that conversation are not on record, but they must have been of this kind: "There is some misunderstanding here. My brother was not trying to steal from the company." When the internal audit director again discussed the matter with his boss, the controller, he heard a different tune. The controller told the auditor he had misconstrued the evidence, making more of it than he should. The

right solution was simply to tell this sales manager to be more careful with expense reporting. And the controller warned the auditor: "We don't want you to make these kinds of mistakes in the future."

End of story? The auditor knew that there was still an issue and put it on the audit committee's agenda. Sitting down with the committee, he did not realize that the controller had prereported the issue and altered the facts to make them seem innocuous. "Why would you even bring this up with us?" a committee member asked. "We're not interested." The result was just what his adversaries had expected: The internal audit director came off as seeming to have poor judgment.

What options remained for this embattled director of internal audit? Choosing not to endanger his job by stepping completely around the chain of command, he preferred to live to fight another day—to fight some other issue, not this one.

Are scenarios of this kind rare in the professional lives of internal auditors who take their fraud detection responsibility seriously? Unfortunately, they probably are not rare, and they point out a measure of the challenge of integrity and skill facing internal auditors.

Hitting the Jackpot in the Gaming Industry

It does not take much intuition to recognize that the gaming industry needs an especially strong internal audit function. Like financial services, the gaming industry is all about money, but it is also about hospitality, entertainment, transportation, and the unobtrusive policing of large numbers of pumped-up, excited people having a good time.

A senior internal auditor was invited to a meeting of casino executives to discuss the controls that would be needed around a new marketing program, initiated by the vice president of marketing, who was present at the meeting. This entrepreneurial executive was widely admired at the casino as the largest revenue producer in the managerial ranks. His reach extended far. In fact, he had a second business of his own, in partnership with the casino: a junket business that transported tourists and games players by bus and air to the casino for a day or more of enjoyment. Now he was proposing a new tour and travel program to increase traffic to the casino—and incidentally, generate a third stream of income for himself, personally.

While the internal auditor participating in the meeting had been summoned on a narrow agenda—to recommend controls for the proposed business—he found himself feeling uneasy about the whole picture. Something did not seem right. With senior management's authorization, he teamed with forensic accounting investigators, and together they launched a discreet investigation that probed the accounts for which the vice president was responsible, both in the core casino business and in the related junket business.

The result was astonishing. The executive was stealing from the company in some 15 to 20 different ways. Some of the schemes were primitive. For example, by using inflated foreign exchange rates, he cheated to the tune of tens of thousands of dollars in his expense reports. In that particular scheme, he made a mistake that should have been detected much earlier: The exchange rates he reported were preprinted on the forms he used, but foreign exchange rates vary over time. Other schemes were sophisticated. Because he had significant influence over casino credit-granting and credit write-off decisions, he was able to put credit in the hands of people who were

in reality not creditworthy and then authorize the write-offs, which amounted over time to many millions of dollars. The investigation did not prove whether he had profited directly from that process, but all indications were that he had. In the junket business, he also had a lucrative scheme underway, which involved buying airline tickets for his customers at the highest possible price, collecting the 10 percent travel agency commission, and then billing through to the casino company the full value of the ticket. This pattern, like much else, was undisclosed.

There was much more. This individual was a true maestro of fraud. For example, he had fraudulently arranged for the casino to pay the salary and benefits of the personnel working in his travel agency. He was billing the casino for housekeeping services at his own business offices and leasing for $12,000 a year—again, at the casino's expense—a desktop computer system that could have been purchased for $2,000. The lease was held by his outside accountant, who was also his landlord. And on and on—nearly everything he touched proved on investigation to have some element of fraud. The company's losses were at the level of many millions of dollars.

What became of him? He was not immediately terminated, because the state division of gaming enforcement had been conducting its own covert investigation and wanted to follow his movements while imperceptibly restricting his ability to perpetrate further fraud. For this reason, the state authorities chose the time of his dismissal. He actually went on to enjoy 15 minutes of notoriety when he was called to testify before a Senate committee investigating infiltration by foreign organized crime organizations into the U.S. gaming industry. The internal auditors at the company wound up their work by calculating that for every dollar of revenue this man had brought to the casino door through legitimate marketing activities, he had cost the company $1.07 million. It is worth noting that this consummate fraudster fit the profile of the white collar criminal described in Chapter 2. He resembled any number of executives you might see walking down the streets of any major financial district. It could have taken many more years to expose him if the senior internal auditor called in to discuss controls had not felt uneasy as he listened. This was a victory for professional skepticism and experience.

REPORTING RELATIONSHIPS: A KEY TO EMPOWERING FRAUD DETECTION

Fraud detection as a task for internal audit comprises both a mission and a skill set, supported by an attitude of professional skepticism and the cumulative experience of the practitioner. However, it does not exist in a vacuum: It needs the right organizational support to be fully effective. For this reason, the issue of reporting relationships is more important than one might think.

The appropriate reporting lines for the internal auditors are critical to achieve the requisite independence, objectivity, and organizational stature needed to effectively assess the organization's internal control, risk management, and governance processes.[9] As a general rule, internal audit reports to the audit committee, with an

[9] Institute of Internal Auditors Research Foundation, "Internal Audit FAQs: What is the Appropriate Relationship between the Internal Audit Activity and the Audit Committee?" www.theiia.org/theiia/about-the-profession/internal-audit-faqs/?i = 1082.

administrative or dotted-line report to the CFO. In 2003, the Institute of Internal Auditors (IIA) endorsed two reporting relations, the first described as functional (to the audit committee), and the second as administrative (to the CFO, controller, in-house legal counsel, or, in a few instances, the CEO).[10] A 2007 study indicates that 47 percent of internal audit units report administratively to the CFO or office of the CFO.[11] However, the majority of respondents in a recent study examining the future of internal auditing in 2012 anticipate an increase in the number of internal audit functions reporting administratively to the CEO rather than the CFO, a common benchmark of the relative independence of an internal audit group.[12] In certain industries, notably banking and casinos, regulators now explicitly require internal audit to report to the audit committee to better ensure the independence and integrity of the function. In the post-Enron, post-WorldCom era, a number of powerful federal agencies, including the Federal Reserve Board and the Office of the Comptroller of the Currency, stated, "Internal audit should report to the audit committee—and if not, we're going to criticize you." But a forceful statement from a powerful agency is not a binding law. Except in a handful of industries, the reporting relation of internal audit remains a management decision.

Even if, as in the majority of cases, the director of internal audit reports functionally to the audit committee, that director will meet with the committee some four times annually and with the CFO much more frequently in the normal course of business. The CFO will naturally exercise a great deal of authority over the scope of internal audit projects and monitor the results and recommendations that flow from them. Although there is nothing improper in this, as a best practice, the internal auditor should report directly to the audit committee or its equivalent.[13] The quality of the relationship between internal audit and the audit committee depends on effective communications.[14] One study described a wide range of communication techniques being employed by internal audit leaders to foster good relations with their audit committees, which included: conducting private sessions with their audit committees on a quarterly or more frequent basis, having open lines of communication with their audit committee chairs, helping set the audit committee agenda, providing their audit committees with information that extended beyond internal audit reports, and facilitating periodic discussions with their audit committees on key risk topics.[15]

With assured and unencumbered access to both the CFO and the audit committee—and even though, given human nature, such difficulties can never be eliminated entirely—some of the difficulties internal auditors experience and that we

[10] Institute of Internal Auditors Research Foundation, *Internal Audit Reporting Relationships: Serving Two Masters* (Altamonte Springs, FL: Institute of Internal Auditors, 2003), 8.
[11] PricewaterhouseCoopers, "2007 State of the Internal Audit Profession Study: Pressures Build for Continual Focus on Risk," 42. According to this report, "31 percent report to the CEO or president."
[12] PricewaterhouseCoopers, "Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-Centric Approach," (2007), 41.
[13] Id.
[14] PricewaterhouseCoopers, "2008 State of the Internal Audit Profession Study: Targeting Key Threats and Changing Expectations to Deliver Greater Value," 7.
[15] Id.

have explored through case studies likely would be reduced, but that will ensue only if all stakeholders in the internal audit process reach for a new level of excellence.

Let us be clear about what we mean. Internal auditors should improve their fraud detection skills and should program fraud detection explicitly into their work plans. Internal auditors also should be ready to exercise integrity and courage when the situation calls for it. Dual reporting lines, if they are active and reliable, can support their willingness, when necessary, to tell truth to power. The needed truth may be as simple as these words to the CFO: "I think we should still audit X this year. The risks merit it. Let's leave it in the annual work plan." It is not too much to say that internal auditors face both pressure to disregard areas in which they conscientiously know that work is needed and pressure to overlook, minimize, or reinterpret suspicious facts they have uncovered. The internal audit function can be only as good as the audit committee and senior management want it to be.

TOMORROW'S INTERNAL AUDITOR, TOMORROW'S MANAGEMENT AND BOARD

All internal auditors will be expected to exercise a higher degree of professional skepticism, to ask the next question and the next, and to corroborate audit evidence rather than accept a single informant's word. The internal auditor's focus on fraud detection should be explicit and methodical.

The case studies in this chapter make clear that professional skepticism and training in fraud detection are not enough. Internal auditors will on occasion need courage and unshakable integrity to challenge others and their assertions. These can be difficult situations. This observation brings to light the continuing need for management and the audit committee also to play their roles effectively, proactively, and with integrity.

Management must be willing to invest in fraud detection through the internal audit team and to feel that the money is well spent even if the internal audit director reports as follows: "Mr./Ms. CFO, I'm delighted to tell you that we spent 500 hours this year specifically testing for fraud in major risk areas, and we found *nothing*. To the best of our knowledge, this company is free of significant fraud." Management must come to view this as good news rather than as a pretext for cutting back on internal audit's budget in the next fiscal year.

The audit committee, now and in the future, needs to view itself as the ultimate boss and beneficiary of internal audit's activity. Its members must be sensitive to management's agenda for the internal audit and recommend modifications when they perceive the possibility of insufficiently monitored risk to the company's finances and operations. The audit committee must position itself as independent of management whenever there is any doubt about matters of integrity, accountability, and transparency—and as enthusiastically supportive of management when management is doing its job well.

Genuine cooperation across this network of participants—internal auditors, senior executives, and the audit committee—goes a long way toward ensuring that when external auditors examine a company's internal controls and financial reporting, they will be better able to do their job.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 7

Teaming with Forensic Accounting Investigators

Erik Skramstad

Forensic accounting investigators can make significant contributions to a financial crime investigation provided that they can work effectively with the company's internal and external auditors as well as with other constituents involved in resolving allegations or suspicions of fraud. In addition to a thorough knowledge of accounting and auditing, the forensic accounting investigator brings to bear a variety of skills, including interviewing, data mining, and analysis. Some auditors assume that auditing more transactions, with the use of standard procedures, increases the likelihood that fraud will be found. While this can prove to be true in some cases, when there is suspicion of fraud the introduction of competent forensic accounting investigators may be more likely to resolve the issue. This chapter explores how forensic accounting investigators can work effectively with internal and external auditors and considers the interests of other parties to an investigation.

Forensic accounting investigators work in a highly charged atmosphere and often present their findings in forums ranging from the boardroom and the courtroom to hearings before government agencies such as the U.S. Securities and Exchange Commission (SEC). Within the boundaries of an investigation, they typically deal with numerous constituencies, each with a different interest and each viewing the situation from a different perspective. These parties to the investigation may well attempt to influence the investigative process, favor their individual concerns, and react to events and findings in terms of individual biases. Forensic accounting investigators thus often have the task of conveying to all constituencies that the results of the investigation will be more reliable if all participants and interested parties work together and contribute their specific expertise or insight with truth-seeking objectivity. In the highly charged environment created by a financial crime investigation, the forensic accounting investigator usually bears much responsibility for displaying and encouraging levelheadedness.

All parties with a stake in the process—management, audit committee, auditors, and legal counsel—should consider including forensic accounting investigators in the process of decision making about the investigation. One of the key decisions, usually, is the degree to which the forensic accounting investigators can work with and rely on the work of others—specifically, the internal and external auditors. Another common decision is whether forensic accounting investigators—with their

knowledge of accounting systems, controls, and typical fraud schemes—may be added to the team that evaluates the organization's business processes to strengthen the controls that allowed the fraud to occur.

Management may at first be inclined to push for a quick result because it feels the company will be further damaged if it continues to operate under a shadow. Senior executives may be unable, or in some cases, unwilling to see the full scope of issues and may attempt to limit the investigation—sometimes as a matter of self-protection—or they may seek to persuade the forensic accounting investigators that the issues at hand are immaterial. Whatever happened, it happened on their watch, and they may understandably be very sensitive to the forensic accounting investigators' intrusion into their domain. Any defensiveness on the part of management should be defused as quickly and as thoroughly as possible, usually through empathy and consideration on the part of the forensic accounting investigators. The party or entity engaging the forensic accounting investigators—for example, audit committee, management, or counsel—may be committed to a thorough investigation of all issues and is ultimately responsible for the investigation. The committee may engage forensic accounting investigators directly and look to them for guidance, or it may ask outside counsel to engage forensic accounting investigators, who usually will work at counsel's direction in fulfilling counsel's responsibilities to the audit committee. In some cases, the audit committee may need to work with two forensic accounting teams. One team, deployed by the external audit firm, gets charged with assisting the external auditors to meet their 10A responsibilities and provide advice on the adequacy of the investigation conducted by the company.[1] The other team, engaged by 10A counsel, is responsible for an investigation that assists counsel and the audit committee in determining whether there was an illegal act and, if so, what remedial action is needed. Many audit committees recognize that simply reauditing the suspect areas is unlikely to resolve the issues. They are also likely to realize that an overzealous witch hunt may alienate management and employees by implying loss of confidence in their competence or integrity. And deadlines—either self-imposed or imposed by a third party—such as a looming earnings release or regulatory filing may place significant pressure on the investigation. Amid all of these pressures, forensic accounting investigators should keep in mind the goals of all constituents yet conduct a dispassionate, objective, and balanced investigation that is, to the best of their ability, on time and on target.

Internal auditors are enjoying a resurgence of respect in response to additional regulatory requirements and the public outcry for better governance (see Chapter 6 for a discussion of the internal audit function). Many companies are strengthening their internal audit functions, which vary in size, scope, focus, and effectiveness from one organization to another. Internal audit functions may be large or small, compliance based or consultative, executive or operational. Some internal audit units are powerful, with fully functioning administrations and a key voice at high levels, while others are less so. The practice of internal auditing experienced significant change—in light of the Sarbanes-Oxley Act of 2002 and the enactment of voluntary standards by the Institute of Internal Auditors (IIA). For forensic accounting

[1] See footnote 6 in Chapter 5 regarding 10A and its reference to the independence of the external auditors.

investigators, cooperating with internal auditors should be planned in a way that reflects the role of internal audit within the organization.

FORENSIC ACCOUNTING INVESTIGATORS' COOPERATION WITH INTERNAL AUDITORS

As we discussed at greater length in Chapter 6, internal auditors bring a great deal to the table when there are concerns about financial fraud. However, for reasons explained in Chapter 6, most internal audit groups do not have a subgroup of forensic investigators. As such, outside forensic investigators are typically hired to assist internal audit conduct investigations. We have found in the majority of our experiences that teaming with internal audit enhances both the efficiency and effectiveness of the investigation: Internal audit knows the company and its personnel and systems better than outside forensic investigators, which causes the investigation to be more targeted.

While it is ideal to work with internal audit in conducting investigations, it is important that a number of factors (explored later) be considered by those assigned the responsibility of conducting an internal investigation—usually the audit committee.

Internal Audit's Position and Function

Note the group's position in the company's organizational chart and its actual, day-to-day role—which due to any number of factors may differ from the role implied by the organizational chart. For example, internal audit's function and reporting relationship may have, by necessity, been diverted in the period following the enactment of the Sarbanes-Oxley Act, wherein companies were working to document and assess financial reporting internal control structures as required by the Act. Begin this assessment with a look at the mission and charter of the internal audit unit. If possible, consider the way in which the internal auditor is measured by the company with respect to coverage, number of locations visited, types of issues raised, financial savings, and improvements to operating metrics. Among the considerations are the following:

- Is the internal audit unit focused on controls assurance—typically evidenced by location-based or compliance auditing—or on controls consulting, typically evidenced by forward-looking projects, early involvement in system deployments, and so on?
- Does the internal audit plan comply with IIA standards for a risk-based approach—usually in the form of a risk assessment?[2] A coverage-based metric, such as a site visit to every location every three years, is evidence that risk is not the primary driver.

[2] Institute of Internal Auditors, Standards for the Professional Practice of Internal Auditing, § 2010, "Planning: The chief audit executive should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals."

- Are any internal auditors trained in forensic investigative accounting? How experienced are they? Do they provide for a separate and distinct group of investigators? When fraud is suspected, do the internal auditors conduct investigations by means of this specialized group of forensic accounting investigators, or do they use auditors already assigned to the particular project?
- Is there consensus about the role of the internal audit unit within the organization?
- Are internal audit's recommendations implemented, and if not, why not?

All internal audit units must grapple with the issues of independence and conflict of interest. The auditors cannot fulfill their obligations without independence of mind and action, but the types of work they perform call for coordination with operational management. This is a balancing act, and it can often generate tension. How much of the internal audit budget is available to auditors at their own discretion? Are the audit strategic plan and budget developed by the auditors themselves, or are they heavily influenced by the chief financial officer? Has the internal audit unit aided in forensic investigations in the past? Experienced auditors are likely to understand the imperatives and the required mind-set, while inexperienced auditors, however skilled in other elements of internal auditing, may require a strong lead throughout the investigation. A high degree of correlation usually exists between the level of empowerment granted to the individual and the independence and effectiveness of that individual's performance. Many internal audit units are oriented toward compliance or operational efficiency and not financial crime investigation. Internal reporting relationships and organizational tone may either enhance or severely limit the effectiveness of the internal audit unit. Most often, the formal report is made to the audit committee, but there may be an administrative reporting relationship with the finance function. Further considerations: How is the auditor evaluated and by whom? What degree of interaction exists between the internal audit group and the audit committee? Do the two meet frequently and discuss matters in depth, or do they meet only at several formal meetings a year?

Resource Models

The internal audit unit's mission also usually drives operational issues such as the resource model, annual budget, and auditing plan. Among the questions and issues that normally need to be considered in an evaluation of the resource model are the following.

- Whom does the internal audit group principally hire: accounting and control specialists, certified fraud examiners, certified public accountants (CPAs), MBAs, new or experienced people, internal recruits?[3]

[3] When staffing an internal audit unit whose mission emphasizes consulting activities, the human resources department of a company may bring MBAs rather than CPAs on board. However, the MBA skill set may not be as valuable to a forensic accounting investigation as fundamental auditing experience and the ability to understand how financial transactions are recorded.

- How are the internal auditors trained? Is their career path restricted to accounting and controls, or does it enter into operational areas of the company? Do internal auditors rotate through internal auditing and then move to other positions in the company? While benefiting the rest of the organization, such a practice may be counterproductive to building a deep skill set of forensic investigation abilities within the internal audit group.
- Whether the internal audit draws entirely on in-house resources or is co-sourced is not a significant issue unless the views of the co-sourcing partner differ on methodology, tools, and approach. These issues should be considered in a determination of what support is available, together with the contractual arrangements with the co-sourcing partner. Co-sourcing is usually done for one of two reasons: to fill gaps or to build a function. The company may have an internal audit unit but lack specialized information technology resources and therefore looks to a co-source provider. Building a function involves obtaining a capability quickly while providing knowledge transfer from outside forensic accounting investigators to company employees. On one hand, when the co-source partner is filling gaps, the mission, direction, and sometimes the supervision of day-to-day work are in most cases controlled predominantly by the company. On the other hand, when the co-source partner has been hired to build or reengineer the function, the company normally sets the mission and overall direction, but the co-source provider usually exercises tactical leadership.

Working Together

After gaining a thorough understanding of the factors discussed earlier, consider ways in which the investigative team can best work with the internal auditor and be prepared to make recommendations to the audit committee. Each group brings different skills to the task, and the best solution is usually one that incorporates both working together. The internal auditors usually bring:

- *Core skills in auditing:* Collecting and corroborating documentation, sampling, interviewing, and testing and analyzing data
- *Core skills in project management:* Planning, scheduling, document management, creating audit steps (including follow-up), managing issue resolution, and recording and communicating results
- *Knowledge of the company and systems:* Organizational structure, how transactions take place, how errors are likely to evidence themselves, and the strengths of the company's people, systems, and processes

With these competencies, the internal auditor is very well positioned to obtain background information on people, systems, and processes. Past audits may provide insight. The auditor is also a valuable team member in collecting data or serving as an advisor to the forensic investigators on matters of approach, specific issues that come to light, and potential follow-up actions.

At the same time, all parties should acknowledge that normal auditing protocols do not apply. Sending out announcements of visits and advance requests for documentation may not be consistent with the objectives of a forensic accounting investigation. The internal auditors' cumulative knowledge of the company can be

a powerful frontline force in detection and deterrence. Bear in mind, however, that knowledge of the entity can cut both ways: as an efficient jump start or as a set of assumptions that may hinder objective investigation.

The audit committee or whoever carries ultimate responsibility for the investigation might choose to have it conducted without input from or reliance upon internal resources. The forensic accounting investigator may be asked for input into this decision and should be prepared to respond appropriately. The foregoing discussion of factors to consider may be helpful for all parties involved in conducting investigations.

FORENSIC ACCOUNTING INVESTIGATORS' COOPERATION WITH EXTERNAL AUDITORS

The external auditors of a company are commonly engaged to perform an audit under Generally Accepted Auditing Standards, and the primary focus of those external auditors is on auditing the financial statements in compliance with professional standards. How well forensic accounting investigators interact with external auditors typically depends on several factors, including the following.

Client History

The external auditor may be a trusted advisor or may have a strained relationship with the company owing to previous events. Because the forensic accounting investigator is often placed between the company and its external auditor during an investigation, understanding their current relationship is likely to be critical to successful communication during an investigation.

Because external auditors likely know the company better than a newly appointed team of attorneys and forensic accounting investigators, selected in part because of their limited prior experience with the company, they may be very useful sources of information. The audit firm's knowledge about a company's areas of risk, business processes, documentation, systems, and personnel can get the investigative team off to a fast start. The forensic accounting team will also be able to use the auditor's working papers and audit staff to assist in gaining an understanding of the client's systems, culture, and personnel, as well as other important data. Gaining access to information contained in the working papers of the external auditors may require formal access letters, the terms of which should be carefully considered by counsel. Also, the process of obtaining access letters may often take time away from getting the investigation started promptly.

There are situations permitted by law and professional standards wherein an audit committee may retain a forensic accounting team from the external auditor's firm. Considerations in choosing this option include timing, knowledge of the company's accounts, systems, personnel, and industry specifics. Relying on a forensic team from the external auditors has an added benefit: The audit firm and hence its forensic accounting team are independent, whereas the other immediately available resources, such as the internal audit team or the company's general counsel's office, are not. A discussion of the rules allowing these services is found in Chapter 11

(see the discussion surrounding our commentary regarding Rule 2–01(c)(4)(x) of Regulation S-X and Exchange Act Rule 10A-2).

Note, however, that the nature of the allegations or certain external events such as the commencement of a lawsuit or a regulatory investigation may require the audit committee to insist on several degrees of separation between the external auditors and the investigative team—especially if the cry "Where were the auditors?" has already been raised.

The External Auditor in Today's Environment

To meet capital markets' expectations that financial statements must not be tainted with material fraud and in compliance with the regulatory requirements of Sarbanes-Oxley, the external auditor will be involved to some extent in most investigations. This is particularly so in situations involving allegations that the financial statements may have been affected by an illegal act. Any investigation to assess this concern will likely be conducted by the audit committee, the process and results of which will be closely monitored by the auditors in accordance with their responsibilities under professional standards and 10A of the Exchange Act. Many external auditors will not complete their audit fieldwork until the investigation is complete and they have access to the findings and the company's remedial action plan.

Recognizing the responsibilities of the auditor, the investigation team (counsel and forensic accounting investigator) may consider asking for input from the external auditor early on in the investigation. If there is a disagreement with the external auditor on scope, approach, or procedure, the forensic accounting investigator should find that out earlier rather than later and work through the issues raised. The work and findings of the 10A counsel team cannot be kept entirely from review by the external auditors. While 10A counsel and their forensic team may draw certain boundaries around work relating to legal advice and other matters of privilege, it is generally best to include the external auditors in significant aspects of the investigation with periodic reports. Without this level of cooperation, time to complete the financial statement audit once the investigation is completed may be extended while the audit partner digests the findings, establishes the scope of and carries out related audit work, and evaluates the remedial actions, control implications, and financial statement disclosures.

Invariably, the question of the attorney work product and attorney–client privileges arises when the question of sharing the findings of the investigation gets discussed. This is a complex question and the subject of evolving law. Accordingly, audit committees, auditors, and forensic accounting investigators should be prepared to evaluate the specific circumstances of each situation with counsel before reaching a conclusion. It must be recognized, however, that the external auditor has a legitimate need for fully comprehending the scope, findings, and remedial actions taken as a result of the investigation, which may, under certain circumstances, implicate the privileged nature of certain aspects of the investigation. Auditors are generally well advised to inquire at both the beginning and the end of an investigation as to whether any material either will be or has been withheld from them because of privilege issues. It may be simplest for the auditors to tell the audit committee, with its 10A counsel present, that they need to be informed at any point in the investigation when the privilege is being asserted.

OBJECTIVES OF ALL INTERESTED PARTIES

The forensic accounting investigator must bring independence and objectivity to the investigation and recognize the objectives of each of the interested parties to the investigation.

Forensic Accounting Investigators' Objectives

Forensic accounting investigators' objectives are determined by the scope of work and the desire to meet the goals of whoever retained their services. Regardless of the differing interests of the various constituencies, forensic accounting investigators must typically answer the following questions:

- Who is involved?
- Could there be co-conspirators?
- Was the perpetrator instructed by a higher supervisor not currently a target of the investigation?
- How much is at issue or what is the total impact on the financial statements?
- Over what period of time did this occur?
- Have we identified all material schemes?
- How did this happen?
- How was it identified, and could it have been detected earlier?
- What can be done to deter a recurrence?

Forensic accounting investigators should always keep in mind that they are primarily fact finders and not typically engaged to reach or provide conclusions—or, more formally, opinions.[4] This differs from the financial auditor's role, as often noted in previous chapters. The financial auditor is presented with the books and records to be audited and determines the nature, extent, and timing of audit procedures. On one hand, the financial statements are management's responsibility, and an auditor confirms they have been prepared in accordance with Generally Accepted Accounting Principles after completing these procedures and assessing the results. The forensic accounting investigator, on the other hand, commands a different set of skills and works at the direction of an employer that may be management, the audit committee, counsel, or the auditing firm itself.

The selection of audit procedures is judgmental and an integral part of the audit team's responsibilities. Not surprisingly, when auditors choose to enlist the services of subject matter experts such as forensic accounting investigators, they expect the investigators to offer suggestions on appropriate procedures to be performed as well as related costs, risks, and expected outcomes. The investigators should be careful

[4] The exception is that in civil litigation, a forensic accountant may be asked to opine on the existence of fraud under the civil evidence standards, wherein the existence of a tort is based on a preponderance of the evidence, as opposed to the stricter criminal evidence standard of "beyond a reasonable doubt." A forensic accountant who is asked for an opinion takes on elements of the role of auditor and must determine whether the nature, scope, and timing of the procedures were or are sufficient.

not to execute such procedures unless specifically asked to do so by the audit team (or whoever is directing the investigators). This approach can lead to frustration on the part of the investigators if, during an investigation, forensic accounting investigators are ordered to stop and in effect put down their pencils. Should that situation occur, it may be entirely appropriate to discuss their concerns with the audit team. But keep in mind that the audit team is generally more knowledgeable about the client's business as well as other audit procedures that may mitigate the forensic investigator's concerns. In extreme cases, it may be appropriate to resign in protest, an eventuality discussed in more detail later. But the forensic accounting investigators should take direction from those who engage them, as requested, be they auditors, directors, or counsel.

Objectives of Other Parties to the Investigation

During an investigation, each interested party may view the same facts differently. For this reason, it is important to understand the likely biases and goals of all stakeholders and to view, in a broad context of expected and quite naturally differing points of view, any conflicts that may emerge.

Management understandably may be eager to bring the investigation to a quick conclusion. The chief financial officer may be defensive over being seen as having "allowed this to happen" to his organization. The CEO may be concerned about the investigation's impact on share price, company reputation and liability, and employee morale. Perhaps citing cost or scope issues—but likely more concerned about staying as close as possible to events as they unfold in the interest of no surprises—management's overall reaction may be to tightly manage the investigation.

The *board of directors,* through the independent members of its audit committee, is likely to focus on conducting a thorough and complete investigation, but its members may lack the experience needed to assess the effort. Also, they may be concerned about their personal reputations and liability. The board is likely to look to legal counsel and in some cases to forensic accounting investigators to define the parameters of the project.

Regulatory agencies, including the SEC and law enforcement agencies such as the U.S. Department of Justice (DOJ), have enforcement and prosecutorial objectives beyond the scope of the investigative team's objectives.

Counsel will act in the best legal interests of its client, which could be the management team, the audit committee, or other directors, with the exception of counsel engaged to conduct a 10A investigation. Such 10A counsel must conduct an independent investigation free of the advocacy role required of counsel engaged to prepare a defense of the company in a pending civil litigation, or DOJ or SEC or other regulatory agency investigation. The role required of forensic accounting investigators by the legal team may vary, depending on the team's needs. As such, the forensic accountants should not expect to participate in all activities typical of financial crime investigations. For example, the legal team may or may not see a need to include the forensic accountants in all interviews, favoring instead to have them attend only those interviews in which the legal team expects accounting issues to surface. In most investigations in which counsel is involved, they are responsible for the conduct of the investigations and will assign and allocate resources accordingly.

The *internal auditor* may have a variety of objectives, including not alienating management, staying on schedule to complete the annual audit plan, and not opening the internal audit team to criticism. The internal audit team may also feel embarrassed, angry, and defensive that it did not detect the wrongdoing.

The *external auditor* may have several concerns, including whether the investigation team will conduct an investigation of adequate scope, whether the situation suggests retaining forensic accountants from the auditors' firm, whether forensic accountants should be added to the audit team, and even whether the investigation will implicate the quality of past audits.[5] The concerns on this front are complex.

Registered independent accounting and auditing firms are good places to look for forensic accounting investigators. However, in light of the requirements of the Sarbanes-Oxley Act, in some circumstances the external auditors may not be engaged, and additionally, when they can be engaged, some audit committees are nevertheless averse to engaging forensic professionals from their external auditing firm. This may be the correct decision, although not in every case. (See Chapter 11 for further discussion.)

Also, there will likely be situations in which auditors may elect to consult with a forensic accounting investigator from their own firm regarding the proposed scope or method of an investigation being conducted at an audit client.[6] For example, the law firm conducting a 10A investigation may decide not to conduct an e-mail review as part of its investigation. This decision may or may not be appropriate. Consultation with a forensic accounting investigator may assist the audit partner and the partner's team in assessing the scope of investigation either proposed or performed. As an example of a detailed issue pertaining to scope, in some investigations e-mail is obtained by copying the relevant server files. The audit firm's forensic team might suggest that hard drives found on personal computers, portable mass storage devices like flash drives, personal digital assistants, and the like be *imaged* instead of simply copied, so that files not retained on the servers as well as deleted files are captured.

Audit partners may use their firm's forensic accounting investigators to assist in a variety of ways, including:

- Receiving detailed reports of questions and facts discovered by 10A counsel. Attending selected interviews with 10A counsel or counsel's forensic accounting advisors may be appropriate in some situations as well.
- Additional document review—which may include an e-mail review—or expanding the audit tests of certain accounts.
- Attending update meetings called by 10A counsel to advise on the progress of an investigation.

If the forensic accounting investigators are from the audit firm, the firm may expect to be involved in the procedures and findings at every stage. Some counsel and boards view this as a barrier to hiring the audit firm's forensic accounting investigator

[5] See Chapter 5 regarding specific requirements of the auditor under Section 10A of the Exchange Act.
[6] Id.

to conduct the investigation; no matter who completes the investigation, however, critical information must still be communicated to the auditors.

Stockholders may become concerned once suggestions of financial impropriety surface. They may file a class-action lawsuit with the objective of extracting the largest possible settlement from the company and other parties, including the external auditors.

The company's *lenders* are likely to be concerned about their exposure to losses. The investigation may take place during a period of financing negotiations and may therefore need to address the lenders' objectives.

The *public at large* may feel some degree of vested interest in the investigation, particularly if the entity is a public, quasi-public, or charitable organization or if it is a significant regional employer. These concerns are often reflected in and fed by media attention, and they create pressure to "get to the bottom quickly."

HOW SHOULD THE INVESTIGATION OBJECTIVES BE DEFINED?

Forensic accounting investigators should develop a plan that offers the client investigative alternatives. The investigation should obviously focus on the facts that cause concern, with the ultimate objective of determining if an illegal act has been committed. In their quest to achieve the objectives of the investigation, forensic accounting investigators must be mindful that they are governed by the ethical principles and other guidelines of the authoritative professional organization(s) to which they belong—be it the American Institute of Certified Public Accountants, the Association of Certified Fraud Examiners, or both.

The forensic accounting investigator should recognize that auditors may be apprehensive when confronted with issues of fraud—and appropriately so. Sensitivity to auditors' concerns will go a long way toward easing their natural disquiet when it is determined that the company has begun an investigation to evaluate allegations of fraud. Keeping auditors informed in an appropriate manner, agreed to by the client, will help ensure the efficiency of the financial statement audit.

In earlier chapters of this book, the issue of financial statement materiality has been raised more than once. In the course of an audit, numerous immaterial variances and adjustments are identified, documented in the working papers, and never adjusted on the books and records of the company.[7] This is appropriate and consistent with auditing standards. Materiality is a filter that allows the auditors to work efficiently and effectively. In the course of a financial investigation, however, a small fact, immaterial under normal circumstances, may have a critical bearing on the overall investigation.

[7] Historically, materiality has been evaluated primarily by using quantitative measurement standards such as X percent of total assets or net income. In 1999, however, the SEC released Staff Accounting Bulletin 99 (SAB 99), which reemphasized the view that materiality should be evaluated from a qualitative as well as a quantitative standpoint. View at http://www.sec.gov/interps/account/sab99.htm.

WHO SHOULD DIRECT THE INVESTIGATION AND WHY?

A ship has but one captain and, generally, a company's audit committee must proactively lead the investigation. Forensic accounting investigators follow the evidence wherever it leads and communicate their findings to the audit committee or to the committee's designee, such as counsel, whose decisions direct the conduct of the investigation. While the external auditors must be satisfied that the audit committee has directed a proper investigation, they neither direct the investigation nor decide what remedial actions are required by the circumstances. Financial crime investigations are fraught with uncertainty, and a wrong move can produce harmful results. Audit committees recognize the value of consulting with a competent team of advisors, including counsel and forensic accounting investigators. A forensic accounting investigator working for an audit committee that does not seek advice or that interferes with the investigation would be well advised to resign the assignment.

In the course of an investigation, a time may come when the forensic accounting investigator is alone in advocating a certain course of action or series of procedures. Suppose the audit committee interprets whistle-blower allegations as implicating the revenue recognition practices of the company but not policies involving the deferral and amortization of related marketing costs, and the forensic accounting investigator disagrees? What is the forensic accounting investigator to do? The evidence should be the driving force in determining the scope and course of the investigation. On one hand, in situations of this kind, be insistent while following the standards, methodologies, and practices that experience suggests are most appropriate in the circumstances. On the other hand, unlike decisions about the scope of the audit procedures—which rest solely with the auditors—decisions about the adequacy of an investigation's scope rest with the audit committee. Typically, the best and most practical use of a forensic accounting investigator is to conduct sufficient procedures to unambiguously resolve the allegations. This is the clearest outcome of an investigation. There is, of course, another outcome: "We conducted our investigative procedures and noted no evidence of fraud." This may or may not be acceptable, depending upon whether the investigation was robust and thorough. A no-fraud-found result could amount to a comfort level consistent with the objective of the investigation at its outset: that of resolving the allegations. Or, if those who evaluate the outcome of the investigation—such as the auditors or the SEC—conclude that procedures were not robust and thorough, it will be difficult for them to arrive at a satisfactory comfort level with a finding of no fraud. In situations in which a no-fraud finding is the investigative result, the adequacy of the scope is often a key element in justifying the conclusion.

Ideally, the forensic accounting investigator should have significant influence over procedures pertaining to the financial aspects of the investigation. Counsel should obviously take responsibility for the legal aspects of the matter and support the efforts of the forensic accounting investigator by providing appropriate guidance. The audit committee should rely on these and other professionals, but in the end *it is the audit committee's investigation.* The committee must take ownership, albeit with the advice of other parties in the core team that influences the direction of investigation. These may include forensic accounting investigators, legal counsel, internal and external auditors, and possibly others such as a public relations firm. Conferring

early and often is routine in these matters and should be strongly encouraged by the forensic accounting investigator.

READY WHEN NEEDED

While fraud is not an everyday occurrence at most companies, boards and auditing firms should anticipate the need to conduct a financial fraud investigation at some time in the future. To this end, they may establish protocols that ensure that if fraud exists, there is a high probability that it will be identified completely and dealt with in a timely and correct manner.

Companies and auditors alike may gain benefit from considering whether heightened risk of fraud exists and, when there is such a risk, what an appropriate audit response to the heightened risk would be. Once indicators of fraud have been identified, a protocol may be put in place for conducting an investigation. If this planning takes place long before the need for an investigation, the procedures can be vetted by all relevant personnel, including the audit committee, management, the legal department, human resources, risk management, and internal auditors.

The external auditing firm may also want to develop a protocol for handling possible red flags and suspicions of fraud. An auditing firm's basic vision as to how to deploy resources for addressing these concerns would typically address many of the points covered in the sidebar titled Fraud Response Protocol, which appears on page 130.

WHERE TO FIND SKILLED FORENSIC ACCOUNTING INVESTIGATORS

Internal Audit

When the need arises for an investigation within a company, management or in-house counsel might naturally first look for a forensic accounting investigator in the company's internal audit group. Owing to a number of constraints, however, companies and their lawyers often find themselves sooner or later having to look to outside resources. The first and foremost constraint may be a lack of experienced forensic accounting investigators in the internal audit unit. Many companies have the practice of rotating accountants and auditors (as well as other operational disciplines) through their internal audit groups for a variety of reasons. However, rotation makes it difficult to cultivate the deep skill sets of forensic accounting investigation—for example, interviewing skills.

When an investigation is needed, it is best to deploy the most experienced fraud detection experts available. In actual practice, there is often a strong desire to use the internal auditors: They are already on site or nearby, and it would appear to be most cost-effective to engage this internal resource in the investigation. This strategy can be most effective if companies develop groups of forensic accounting investigators within internal audit. In the absence of experienced, in-house forensic accounting investigators, our advice is to look outside the company when the need arises.

Internal auditors need access to the same fraud detection and deterrence skills as outside auditors. They may have robust audit programs to deploy on the traditional preventative, cyclic, or rotational basis, absent any specific concerns about possible fraud. Should someone in the organization express specific concerns, even in a general way, consideration should be given to deploying forensic accounting experts. Because audit committees look to internal auditors as the primary group focused on fraud detection and deterrence, a certain number of internal audit professionals should consider attaining the certified fraud examiner (CFE) designation. When testing identifies any situation in which a suspicion of fraud arises, company policy should provide for consultation with professionals from the organization's risk management and forensic accounting groups.

Building the right investigative team is part of the challenge facing audit committees. The combination of internal and external resources can greatly enhance the investigative effort if undertaken with eyes wide open, with experience as a guide, and with a deliberate approach.

Engaging External Forensic Accounting Investigators

If forensic accounting investigators are unavailable within the company, a variety of professional services firms can provide them. Those firms include:

- The external auditing firm
- Registered independent accounting and auditing firms
- Consulting firms (nonauditing and unregistered)

What are the criteria for choosing among these service providers? Care is, of course, needed. Unfortunately, people sometimes identify themselves as forensic accounting investigators even though they do not have sufficient training and experience. No formal requirements in terms of education, specialized training, or experience help the buyer of these services gain some initial sense of the service provider's real capabilities. The area of forensic accounting investigation has become popular of late, and some firms have added the specialty to their service offerings despite a lack of strongly credentialed, thoroughly experienced professionals. Companies and their lawyers should, therefore, consider quite a range of factors in deciding what type of individual to engage to direct an investigation. The requisite skills and experience appear in the following, by no means exhaustive, list:

- Technical qualifications, including certifications such as certified public accountant and certified fraud examiner
- Experience in forensic accounting investigation, with a track record of successfully and unambiguously resolving allegations
- Global resources
- Forensic technology tools and the experience to deploy them
- The ability to understand complex business transactions and their effects on financial statements
- Knowledge of criminology and the workings of the white collar criminal's mind and methods

- Testimony experience before regulators such as the SEC and DOJ and at deposition or trial
- Forensic interviewing experience
- Ability to work effectively in an unstructured and dynamic environment
- Listening skills and patience
- The ability to approach situations objectively and without bias
- Persistence and the will to ask tough questions and deal with difficult, high-stress situations
- Integrity

Accounting and Auditing Firms

The largest accounting firms have gone through tremendous change in the past decade. The majority of these firms now concentrate on audit, internal audit, tax, and selected special services such as forensic accounting.

Larger firms have a pool of auditors that may be trained to become forensic accounting investigators. As well, they have large client bases and employ individuals who have conducted investigations in virtually every industry. The majority of the larger firms have both national and international operations, with global resources that can be quickly mobilized to put an engagement team in place. Such firms are efficient; they do this type of work day after day.

While the larger firms' assets, resources, and tools are valuable to clients, cost is the biggest drawback to hiring a large firm to design and execute an investigation. However, because of the larger firms' resources, vast industry experience, networking abilities, and well-recognized expertise, some companies find it prudent, despite the higher cost, to access that richer pool of expertise.

Many smaller firms have professionals who may have worked previously in larger firms and who may hold both the CPA and CFE credentials. They may or may not support a core group of people who concentrate exclusively on forensic accounting investigation, but they may nonetheless field professionals with backgrounds similar to those possessed by forensic accounting investigators at larger firms. Although many small forensic accounting firms are judged to be less expensive than the larger firms, they also have a smaller presence across the United States and may have limited or nonexistent access to international resources. These issues are, of course, factors in the selection process. A Midwestern company had a problem in Indonesia and needed investigative resources there without delay. The board first turned to the company's auditor, a large, regional Midwestern firm at which a few individuals performed forensic work. However, U.S. practitioners with the necessary skill set were not available from that firm to travel to Indonesia, and the firm had no Asian offices at all. Under the circumstances, the company decided to engage a Big Four firm, and within 48 hours an Asian investigative team was onsite at the company's Indonesian subsidiary.

Other factors in the selection process may include:

- How the outcome of the investigation may be used—for example, to initiate a legal proceeding, arbitration, or response to the inquiry of a regulatory or law enforcement agency

- Whether the investigation assignment is initiated in response to significant matters, including:
  - Whistle-blower allegations in potential *qui tam* matters
  - Regulatory inquiries
  - Federal subpoenas
  - 10A investigations
  - Foreign Corrupt Practices Act violations
  - Breach of physical security or data security measures

The decision as to whom to engage in a financial crimes investigation is difficult. It should be considered with the thoughtful advice of the board, both inside and outside counsel, and management, internal audit, and risk management directors.

FRAUD RESPONSE PROTOCOL: AUDIT FIRM DEPLOYMENT CONSIDERATIONS

- *Deployment.* Deploying an organization's most experienced fraud detection experts when there is greatest risk to the organization—for example, when a heightened suspicion of fraud has surfaced—ensures that the best resources attack the problem. When suspicions of fraud arise, forensic accounting investigators should be among the professionals considered for deployment.
- *Clarity of roles.* Clarity should be promoted within the organization. Those who deploy the firm's resources in matters in which suspicions of fraud arise should be aware of who in their firm possesses the necessary training and experience to deal with such issues. The distribution of services performed by the firm should be determined by its business unit leaders, which should cover the deployment of those resources charged with forensic accounting investigation. When audit testing, control reviews, or other attestation services identify a situation in which suspicions of fraud arise, it may well be advisable for firms to consider requiring consultation with their risk management group. This group may suggest further consultation with a forensic accounting investigator from the firm's forensic accounting practice. The organization should have a clear policy as to who must be involved when there is a suspicion of fraud (see Chapter 5).
- *Resources.* Alignment of resources having similar skills helps address such issues as training, industry specialization, and accreditation programs. Accordingly, forensic accounting investigators should be aligned within a single business unit just as a firm might recognize other specialists, such as tax specialists, actuaries, and pension specialists. This strategy ensures that all financial crime investigations are performed by a relatively small and specialized group of professionals.
- *Audit team readiness.* Audit team readiness may be enhanced by cultivation of fraud detection skills. While financial statement auditors need not become fully prepared forensic accounting investigators, they will likely have as part of their audit methods certain practices aimed at surfacing suspicious transactions, should they exist, as suggested by SAS 99.

When an investigation into significant allegations is going to be conducted, a variety of parties must team up to ensure the most efficient possible result. These include the board, audit committee, general counsel, management, internal auditors, external auditors, special counsel, and the forensic accounting investigator. Whether or not the forensic accounting investigator is working with independent counsel or is supporting audit colleagues, communication and cooperation generally create substantial efficiencies in the process and help ensure that the expectations of all concerned with the outcome are met.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 8

Anonymous Communications

W. McKay (Mac) Henderson and Peter J. Greaves

An increasingly frequent occurrence in the corporate world is receipt of an anonymous communication[1] that suggests the existence of issues within or affecting an organization and usually relaying a broad range of allegations. Anonymous communications, often called *tips,* may take various forms, including a posted letter, telephone call, fax, or e-mail. In years past, some recipients may have felt comfortable disregarding communications of this type. However, in today's environment such communications are usually taken seriously, and an effort is made to resolve the allegations. By their very nature, such investigations are triggered suddenly and generally require a prompt and decisive response—even if only to establish that the allegations are unfounded or purely mischievous. The allegations may be general statements or they may be very specific, identifying names, documents, situations, transactions, or issues. The initiators of such tips are motivated by a variety of factors, ranging from monetary recovery (substantial monetary recovery is available to whistle-blowers under the U.S. False Claims Act, discussed in later pages), moral outrage, and genuine concern over an issue to the desire of a disgruntled employee to air an issue or undermine a colleague.

While anonymous tips are by no means new phenomena, legislation such as the Dodd-Frank Act of 2010 and the Sarbanes-Oxley Act of 2002, corporate scandals such as Enron and WorldCom, and the increased scrutiny of health care providers and defense contractors through suits under the False Claims Act have served to raise the awareness of whistle-blowers[2] and the importance of anonymous reporting mechanisms. This awareness, coupled with the dismay of some employees and members of the public that there has been a violation of public trust by some large businesses—especially during the credit crisis of 2008 and 2009—has led to an increase in the number of anonymous tips received by both businesses and regulators.

[1] For this chapter, the term *anonymous communication* or *tip* refers to anonymous information received through various media.

[2] In this chapter, we use the term *whistle-blower* generically to refer to any individual providing or submitting an anonymous communication. The term whistle-blower denotes a person who informs against another or reveals something covert. No negative connotation is implied; the individuals involved are often concerned employees raising genuine issues, and in many cases, the entity appreciates their initiatives.

The enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010 is expected to further encourage and protect whistle-blowing and facilitate the trend of increasing numbers of reports. As of this writing the Act's three main sections relating to whistle-blowing (Sections 748, 922, and 1057) are not yet fully operational as the implementing regulations are still within the public comment period.[3] However, Section 922 of the Dodd-Frank Act directs that a program to reward individuals who provide the SEC with information leading to a successful enforcement action be compensated with a monetary reward of not less than 10 percent and no more than 30 percent of the monetary sanctions collected by the SEC.[4] This explicit monetary incentive to encourage whistle-blowing may be a significant change in governance challenges facing public companies.

Faced with the sudden receipt of a tip, and now the potentially greater likelihood of external disclosure to regulators, auditors and executives should rapidly plan and implement an investigation based on a reasoned, tried and tested, and fully case-specific approach to ensure that the interests of all parties are protected. Management should resist the urge not to conduct an investigation because the allegations appear to be groundless. Such an approach may expose the company to unnecessary risk. The allegations should be investigated promptly and effectively. One has only to look at certain terms in the False Claims Act, such as *willful blindness* and *reckless disregard,* to begin to understand the exposures, not the least of which could include having to explain to a corporate board or regulatory body why the company chose to take no action. The failure to act may lead to fines and penalties that might not have been levied if the underlying situation had been addressed appropriately at the outset.

TYPICAL CHARACTERISTICS OF ANONYMOUS TIPS

Anonymous tips come in a wide variety of forms and, as we have said, through quite a number of channels and are addressed to various individuals and groups within the company or to outside entities, government agencies, and even outside news agencies. Recipients within the company may range from legal counsel, audit committee members, senior management, and department supervisors to human resources managers and the compliance or ethics officer. A tip may take the form of a typical business letter addressed to the company,[5] an e-mail (usually from a nontraceable account), or an official internal complaint. It may also duplicate tips submitted to news agencies, competitors, Internet web site postings, chat rooms, or government agencies. Or it may also be a message to an internal ethics hotline number. Whatever form it takes, a tip may contain allegations that are factually correct at its core, although it also may include embellishments or inaccurate information, wildly emotional allegations, or poor grammar. Furthermore, it may be disorganized, repetitive, and display unprioritized thoughts, and in many cases, key issues will be mixed with

[3] See the SEC's proposed Regulation 21F, Securities Exchange Act Release No. 63237, issued November 3, 2010.
[4] See SEC Proposed Rule 17 CFR parts 240.21F-5(a).
[5] In such instances, the letter's postmark is typically nondescript and useless in investigations.

irrelevant matters and unsupported personal opinions. However, while the tip's information about specific issues may not be absolutely correct, it may contain a grain of truth or may identify elements of several unrelated but potentially troubling issues.

In one notable case, an accounting department employee alerted the board of directors regarding his concern that the finance director was ignoring demands from the tax authorities and allowing penalties to accrue. Upon investigation, this proved to be so, but the reasons behind the finance director's actions proved to be of greater concern and indeed led to the bankruptcy of the company: The finance director, in collusion with others, had been inflating the company's performance for a number of years, and this had led to a material overstatement of asset values. The scheme had been perpetuated by borrowing against the fictitious assets, and it unraveled when the level of borrowing failed to cover the funds needed to settle taxes levied on fictitious profits.

In some situations, the allegations aired in an anonymous tip may be known within the company and labeled as rumors or gossip. Some whistle-blowers are neither gossip hounds nor disgruntled employees but, rather, frustrated employees who have tried to inform management about a problem and have gone unheard. Only then do they file a complaint by sending a letter or an e-mail or making a phone call.

While one should never leap to conclusions upon receipt of an anonymous communication, inaction is not a recommended option. One of the dangers of ignoring an anonymous tip is that a situation that can be satisfactorily addressed with prompt action at lower levels or locally within the company may become elevated to higher levels or to third parties and regulatory bodies outside the company because the whistle-blower believes the communication has been shunted aside. This can have damaging consequences for an organization's reputation and brands if the allegations become public or attract media attention and a cover-up appears to have occurred, however well intentioned the organization may have been. Ignoring an anonymous tip also may negatively affect staff morale and motivation, if suspicions of impropriety are widespread among staff and it appears that the employer is uninterested or doing nothing to rectify the situation. Ultimately, management may leave itself open to criticism or perhaps the danger of regulatory censure or legal action by stakeholders or authorities if it cannot demonstrate that it has given due consideration to the issues raised in an anonymous communication.

FEDERAL STATUTES RELATED TO ANONYMOUS REPORTING AND WHISTLE-BLOWER PROTECTIONS

The False Claims Act (FCA),[6] dating from the American Civil War, provides that a private citizen may bring an action against a person or company believed to have violated the law in the performance of a contract with the government. Such actions are brought for "the government as well as the plaintiff" and are referred to as

[6] False Claims Act, 31 U.S.C. § 3729 et seq.

qui tam actions[7] or whistle-blower lawsuits. In such cases, the individual plaintiff is known as a *relator*. The relator can file a lawsuit under seal with the court, to be reviewed by the U.S. Department of Justice (DOJ). If the government, after reviewing the complaint, decides to intervene or join the suit, the complaint may stay under seal for a significant period of time while the government investigates. The government has the right to conduct an investigation with or without notice to the subject entity and may choose not to inform the subject entity until the complaint is unsealed, thereby becoming public information. The FCA provides for payment to whistle-blowers up to a certain percentage of the recovery, ranging from 15 to 25 percent.[8] The FCA also provides for certain protections against retaliatory action against the relator by an entity or individuals. While the FCA focuses primarily on complaints related to violations of government regulations or contracts, it illustrates that private persons can expose events that result in significant liabilities.

WHO DID IT?

Often, the initial impulse of a company is to speculate on who blew the whistle. While such brainstorming can have real benefits in regard to identifying individuals who may have knowledge of the situation and should be interviewed, auditors and executives should be cautioned not to jump to conclusions or speculate to excess, because they may soon be imagining problems everywhere or reading more into statements than the circumstances actually merit. The most important issues at this early stage are not to fasten onto unverified theories or conclusions that may jeopardize the investigation and not to take retaliatory actions against individuals who are suspected whistle-blowers.

After a company received an attention-getting anonymous letter, the forensic accounting investigators assigned to the investigation planned a series of interviews to obtain a basic understanding of the company's operations, processes, controls, and structure. At the early stage of the investigation, the company decided not to disclose the existence of the letter in the course of its interviews. This was out of respect for the confidentiality of the whistle-blower, whose identity was unknown.

In the course of an interview, one individual seemed unusually knowledgeable about many of the accounting, customer information, and record-keeping systems. His position in the company did not call for such extensive knowledge. Probing more with curiosity than with investigative purpose, the interviewer asked how he came to have this knowledge. Could he shed light on other areas? The gentleman immediately became very nervous and from then on, provided cautious answers. The interviewer decided to depart from the interview plan

[7] In a *qui tam* action, the plaintiff sues for the state as well as for himself. *Black's Law Dictionary* provides the Latin original and translation: "qui tam pro domino rege quam pro sic ipso in hoc parte sequitur," meaning, "who as well for the king as for himself sues in this matter."

[8] 31 U.S.C., § 3730 (d).

and asked him whether he was aware of allegations recently raised in a whistle-blower complaint received by the company. He said, "Yes, in a way. I am the whistle-blower."

In situations in which the identity of the whistle-blower becomes known, direct exploration of the whistle-blower's information and perspective may assist the forensic accounting investigator to expedite resolution of the allegations. However, the forensic accounting investigator should proceed with caution in these situations and consult with others. We have encountered situations in which whistle-blowers revealed themselves but thereafter wanted to control the investigation by attempting to insert themselves in the process and evaluate the progress of the forensic accounting investigators.

DOJ used this statute very effectively in the mid-1990s as part of its health care fraud initiative. The number of whistle-blower suits filed that were related to this initiative was in the thousands. *Qui tam* actions sometimes involve current or former employees who become frustrated that a corporation has failed to address their concerns over certain issues. The employees' response is to formalize their complaints and file them under the FCA. All the more reason to take such complaints very seriously.

Another statute that contains mechanisms for anonymous reporting and protections is the Sarbanes-Oxley Act of 2002. As is well known, Sarbanes-Oxley was introduced in response to concerns over corporate governance after the devastating capital markets impact of a series of corporate scandals, including Enron and WorldCom, which resulted in public outcry and calls for increased supervision of public companies. Section 301 of Sarbanes-Oxley requires corporations to have a process in place that encourages, receives, and investigates issues of concern raised by employees. Section 301(4) of Sarbanes-Oxley reads verbatim as follows.

> *Each audit committee shall establish procedures for—*
> *(A) The receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and*
> *(B) The confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.*

In our view, this mechanism is intended to encourage employees to come forward with concerns or to raise their concerns anonymously to the audit committee, which oversees the financial reporting process. Since passage of Sarbanes-Oxley, there has been a steady increase in the number of anonymous tips sent directly to audit committees and independent audit firms. Such tips typically raise several issues and request that the issues be investigated for the good of the company and its stakeholders, including shareholders, employees, and creditors.

Employers are looking for effective ways to receive employee complaints and concerns. While they may have communicated a hotline number that rings to a telephone in the general counsel's office, some employees may perceive that hotline number as not entirely anonymous and may question its effectiveness. While each company may adopt various means to gather the information, ranging from

contracting with outside hotline providers to establishing fax numbers to receive complaints, the key is to provide mechanisms that are free from reprisal and to communicate with and educate employees concerning the means available. We have encountered large organizations that established hotlines but never communicated the existence of those lines to their employees in developing countries and markets—the very places where there is thought to be a higher risk of unauthorized transactions and questionable business practices.

Section 806 of Sarbanes-Oxley (Protection for Employees of Publicly Traded Companies Who Provide Evidence of Fraud[9]) is intended, we believe, to encourage the reporting of potentially fraudulent behavior. The section provides a variety of protections and relief for the whistle-blower in the event of retaliatory action by the whistle-blower's employer. Namely, a whistle-blower employee may not be fired or discriminated against. The employee can seek remedies for such treatment, including reinstatement, back pay, and compensation for special damages.

The passage of expansive whistle-blowing protections in the Dodd-Frank Act continues the trend of broad protections for whistle-blowers. The three main sections that cover whistle-blower activity are Sections 748, 922 and 1057. Section 748 amends the Commodity Exchange Act to prohibit discrimination against an employee for reporting information to the Commodity Futures Trading Commission. Section 922 provides substantial monetary awards to individuals whose whistle-blowing leads to the recovery of monetary sanctions of $1 million of more. Section 1057 includes broad protection to anyone for reporting information to the newly established Bureau of Consumer Financial Protection at the Federal Reserve.

Many believe that the proposed rules, including as they do the potential for monetary awards and the anti-retaliation provisions, will provide a strong incentive for employees and others to bring to the SEC's attention potential violations. We believe the SEC's primary goal in promulgating the proposed rules is to maximize the submission of high-quality whistle-blower information, which appears to be a continuation of the objectives of Section 806 of Sarbanes-Oxley, as an aid to aggressive securities law enforcement. However, this may be double-edged sword. In some cases this may prove to be a positive outcome, providing additional assistance to the SEC in its efforts to detect and deal with securities law violations. Nevertheless, there is a risk that whistle-blowers may bypass internal procedures, ignore internal compliance programs, and go directly to the SEC, undermining corporate governance efforts. Another concern is the loyalty conflict that may be created for individual executives who are members of the inner circle and hold positions of trust. The SEC has made several statements expressing its disinclination to undermine effective internal controls and compliance processes.[10] For example, the proposed rules do provide certain incentives to encourage the use of internal compliance programs by

[9] Sarbanes-Oxley Act of 2002, Public Law 107–204, 107th Cong. 2d sess. (January 23, 2002), § 806: "(a) In General. – Chapter 73 of Title 18, United States Code, is amended by inserting after Section 1514 the following: '§ 1514 A. Civil action to protect against retaliation in fraud cases.' "

[10] 17 CFR Part 240 and 249, Release No. 34–63237 Proposed Rules for Implementing the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, page 4.

allowing whistle-blowers to keep their "place in line" for a monetary award if they first report concerns to the company.

As discussed later in this chapter, most anonymous tips result in some level of investigation and analysis and trigger a variety of concerns. Among them are the external auditor's considerations when encountering anonymous tips as addressed in AS 2 and SAS 99. Additionally, as noted earlier, Sarbanes-Oxley requires audit committees to develop mechanisms to track, investigate, and resolve all allegations of misconduct.

External auditors need to understand the audit committee's complaint-handling process. Whistle-blower communications are likely to arrive through a wide variety of channels. In some cases, these communications may be directed to the external auditor, but in many cases, management, counsel, or the audit committee initially receives them. External auditors may consider such matters as the committee's ability to monitor the completeness of the population of the complaints, with particular emphasis on those relating to financial statement information.

Depending on the nature of the complaints, the external auditor may conduct inquiries in other areas of the company such as risk management, human resources, or divisional management in addition to the audit committee and the company's in-house counsel. Obviously, a cookie-cutter approach cannot be applied for each allegation. The external auditor's response depends on the particular circumstances encountered. In all cases, it would be prudent for external auditors to seek advice of counsel and their own firm's risk management office. If allegations are meritorious and could potentially have a material impact on the company's financial statements, an investigation of some type may be necessary. At that point, the company may decide to retain the services of a forensic accounting investigator to conduct the investigation. If an investigation has already been conducted or is in process, the auditor may want to gain an understanding of the procedures performed to evaluate risk and any potential impact on the financial statements.

The remainder of this chapter addresses the forensic accounting investigator's investigative approach when dealing with an anonymous tip.

RECEIPT OF AN ANONYMOUS COMMUNICATION

Once notified by a client of the receipt of an anonymous tip, the forensic accounting investigator should obtain an understanding of all of the circumstances of that receipt. While the circumstances may appear unremarkable and trivial, that information is often a key factor in determining the best approach to dealing with a tip and, more broadly, often provides clues that are helpful in other areas. Initial facts and circumstances to be established include:

- *How?* This refers to how the information was conveyed—for example, whether it was in a letter, phone call, or e-mail and whether the letter was handwritten or typed. Additionally, the forensic accounting investigator seeks to determine whether the message includes copies of corporate documents or references to specific documents and whether the tip is anonymous, refers to individuals, or is signed.

- *When?* This includes establishing the date on which the message was received by the entity, the date of the tip, and in the case of a letter, the postmark date and postmark location.[11]
- *Where?* This involves establishing where the tip was sent from, be it a post office, overseas, a private residence, within the office, a sender's fax number, or an e-mail account.
- *Who?* To whom was the tip sent? Was it a general reference such as "To whom it may concern"? A specific individual? A department such as the head office or internal audit? The president's office? The press? A competitor? Sometimes an anonymous notification will indicate that another entity has been copied on the document; this requires verification.[12] Always consider the possibility that the tip may have been sent to the auditor or the U.S. Securities and Exchange Commission or both.
- *What?* This refers to understanding the allegations and organizing them by issue. Often, a tip will contain a number of allegations that are variations on the same issue or that link to a common issue. For this reason, it is often helpful to summarize the tip by issues and related subissues. Does the information in the tip contain information that may be known only to a certain location or department? If so, that may point to a group of individuals or former employees as the source of the tip.
- *Why?* What is the possible motivation for the tip? Issues with misreporting financial information? Ethical decisions? Disgruntled employee? Former employee airing grievances?

Assuming that the anonymous tip comes to the attention of the external auditor, a best practice for the external auditor may be to consult with risk management and a forensic accounting investigator to determine whether additional procedures should be performed.

INITIAL UNDERSTANDING OF ALLEGATIONS

The forensic accounting investigator should initially take enough time to understand the allegations. All allegations should be taken seriously but viewed objectively and without preconceptions. The allegations may be close to the truth but not absolutely correct, perhaps owing to the likelihood that the statements are clouded by emotion

[11] This type of background information should be obtained for any communication channel the whistle-blower uses such as e-mail, fax, or voice mail. Computer forensic techniques may assist in analyzing electronic transmission media.

[12] Whistle-blower letters often indicate that they have been copied to various enforcement agencies such as the Department of Justice, the Federal Bureau of Investigation, the Securities and Exchange Commission, or the Department of Defense; to the press, such as newspapers or TV; or to competitors. However, it is often the case that either the letters were not in fact sent to those agencies or the agencies will not confirm receipt of a letter except in the case of a formal notification related to an enforcement action. If the press does receive a letter, the entity is generally able to confirm the same based on queries from reporters.

or limited by the individual's somewhat incomplete grasp of the facts. It is also usually a helpful exercise to consider the possible motivation for the tip (see earlier, *Why?*) and to think through how the alleged activities, actions, or incidents could have occurred. It may be helpful to discuss with the client the nature of business processes in the area of alleged wrongdoing to assess the credibility of the allegations.

DETERMINE WHETHER ANY ALLEGATION REQUIRES IMMEDIATE REMEDIAL ACTION

The initial assessment of the tip should focus on whether or not any aspect of the allegations poses an immediate threat to the safety of employees or property. In a great many whistle-blower situations, this assessment will indicate that the entity must move quickly. The question as to whether the alleged activity may involve criminal or civil liability will also affect the forensic accounting investigators' approach and should be considered carefully in consultation with legal counsel. The investigation should be planned in such a way that if circumstances warrant, immediate actions may be taken to protect the individuals and assets involved and to safeguard the integrity of evidence and information that may be exposed to destruction, alteration, or removal.

In each particular set of circumstances, consideration must be given to the need to protect the identity of the whistle-blower if known or to take steps to ensure the safety and welfare of individuals identified in the tip or otherwise thought to be at risk based on the allegations. Employee welfare issues can range from minor inconveniences and unpleasantness to verbal abuse or, in extreme cases, physical danger. Reducing the physical proximity of those involved is often sufficient—for example, placing individuals on administrative leave or moving them to a different location. In some situations, it may be necessary to consider personal protection by private security providers or even law enforcement agencies. These considerations will differ with circumstances and jurisdiction, and personal safety is a much greater factor in certain territories.

While forensic accounting investigators are not typically expert on personal security matters, they can assist client executives by making them aware of the issues and working with them to obtain advice and assistance from qualified legal, risk management, human resources, and security personnel. Depending on the nature of the allegations, the forensic accounting investigator should advise the client of the potential need to eliminate access to or limit access to buildings or areas and to computer systems so as to eliminate or reduce the loss, damage, or destruction of assets and information. There may be other issues and materials that need to be protected and secured, such as documents, backup tapes, credit card access, bank account access (signature cards, wire transfer authority, check stock, and so forth), offsite storage access, combinations to safes, and passwords to bank accounts and credit cards. To assist with the investigation, obtaining access and securing access to relevant information sources—including but not limited to certain employee files, accounting records, calendars, electronic records, security tapes, phone logs, and expense reports—should be considered to better ensure the physical security of the client's assets. Also, existing security, access to assets by suspected individuals, the nature and portability of assets, and assessment by internal personnel as to the

accuracy of the whistle-blower's allegations all determine the extent of the physical security needed in a particular situation. Even after precautionary measures have been taken, if the target has alliances with employees still onsite, something could slip through the cracks.

Finally, consideration should be given to locating the investigative team in a secured site such as an office with reliable security and to controlling access to documents obtained during the investigation.

DEVELOPMENT AND IMPLEMENTATION OF THE INVESTIGATIVE STRATEGY

The Investigation Team

Upon initial receipt and evaluation of the tip and after decisions on employee safety and asset preservation have been taken, the client, independent counsel,[13] and forensic accounting investigator should discuss the organization and structure of the investigation team and then develop a strategy to address the allegations in the tip. Discretion, speed, and effectiveness are the key considerations in the assembling of a team to respond to the issues created by receipt of an anonymous tip. The team needs to be large enough to address the various issues, but at the outset a small team of experienced professionals is most effective. The team can be expanded as appropriate in the course of assembling a better understanding of the situation.

The use of forensic accounting investigators may not be suitable in some circumstances—for example, harassment matters—but when the allegations suggest financial improprieties, accounting issues, or misappropriation of assets, forensic accounting investigators become critical members of the investigative team. The forensic accounting investigator also may bring interviewing experience, technical skills, and industry expertise to a particular issue or industry sector. The forensic accounting investigator typically works closely with computer forensic specialists to download and analyze electronic information, whether easily available, backed up, or in some cases, deleted. The team may also include individuals from the client company with sufficient authority, corporate knowledge, and independence from the issues and individuals in question to ensure a timely and well-directed approach to the allegations and developments.

A further consideration is control of the team. A typical engagement structure appropriate to many situations is for the audit committee or a special committee of the board to engage an independent counsel. Counsel then engages forensic accounting investigators and other professionals and oversees the assembled team (see Chapter 20).

In most instances, knowledge of the investigation and its progress may be restricted until completion of the investigation or attainment of some other

[13] In engagements of this type, the client often hires independent legal counsel upon receipt of a letter. The independent counsel is usually actively involved because significant legal issues tend to arise (see Chapter 20).

appropriate milestone determined by the investigative team or client. At that stage, a report—preliminary or final, depending on the circumstances—can be made to the board, external authorities, shareholders, or other stakeholders.

DISCLOSURE DECISIONS

An early decision facing the investigative team concerns whether there are any required external or internal disclosures. Addressing the timing and approach for disclosure is a very difficult process. The client should consider obtaining professional risk and crisis management advice, attorney advice regarding legal requirements, and public relations counsel. Forensic accounting investigators are typically aware of the issues surrounding disclosure and can provide valuable insight into the process, but they should refer the client to appropriate professionals for conclusive advice outside of their specific expertise. When the investigation concludes, the issue of disclosure needs to be addressed. Disclosure must be consistent with legal and accounting requirements, regulatory guidance, and any accurate information that investors may already have obtained from other sources. Disclosure can be used on occasion to assist the investigation as a means of gathering information—for example, by tactically inviting media attention or soliciting information from employees on a broad scale. Disclosure is also a signal to regulatory authorities that the company and the board are taking prompt, appropriate, and thorough action, and it is often appropriate to meet with the relevant members of the regulatory community and brief them on the scope and progress of the investigation.

Regardless of the decision on disclosure, the appropriate structure, timing, and format of any notice to employees should be considered and a strategy implemented to minimize rumors on the corporate grapevine due to the presence of external investigators. On one hand, it may be necessary to reveal basic information and confirm the existence of an investigation, although just what is communicated depends on the extent to which it is clear at the time that further investigation is merited. After the first day of interviews, the corporate grapevine typically comes alive. In many situations, the corporate client has a legitimate interest in balancing the natural desire of its employees to understand the details of the investigation against the predictable distraction that the information will cause as employees digest its meaning. On the other hand, that is not the only balancing act: The company will need to protect the privacy of the whistle-blower and its own economic interests while minimizing the adverse effects of the rumor mill. A proactive notice to employees can be very helpful in halting the rumor mill and notifying those with pertinent information to come forward.

Disclosure to the public, including regulators, about the investigation may also be warranted or required. The advice of counsel should be sought in this regard. Consideration also should be given to engaging the company's corporate communications department at an early stage to prepare suitable responses to any unexpected press interest or if public disclosure should become necessary. In significant matters, outside public relations assistance should be sought. Depending on the investigation findings, the company may also need to respond to press inquiries or stories at a later stage.

PRIORITIZE THE ALLEGATIONS

Anonymous tips often include a number of allegations and information presented in a random order, with overlapping issues and issues that initially appear to be unique but later prove to be parts of a larger pattern. The allegations must be carefully sifted to establish those that are potentially genuine and to set priorities for investigation—that is, where the greatest potential problems are in regard to financial loss, physical danger to persons or assets, legal implications, and so on. The forensic accounting investigators need to cut through the verbiage in the tip and separate any personal or judgmental comments from the basic allegations. This should be done systematically, paragraph by paragraph, to map out and agree among the investigating parties as to the principal allegations. The goals of the forensic accounting investigator are to arrange a structure that addresses each issue, to devise a road map to the relevant information, and to consider evidence that will enable the investigation to confirm or refute the allegations.

Once the core allegations have been identified, each one must be understood in the context of the specifics of the business in question, and a plan should be developed to conclude on each allegation. For example, if the first allegation is that an individual has falsified a document, steps should be taken to locate and analyze that document. If the allegation concerns vendor kickbacks, a plan must be developed to investigate, by legal means, any flows of money or gifts between the parties in question, any relationships between the vendor company and the subject company's employees, and those who may be involved at the vendor company.

A key to planning the investigation of each allegation is to grasp how—within the framework of the existing systems, structures, and practices of the organization—the alleged activities could have been carried out. Loopholes and weaknesses in systems help identify switch points at which there were opportunities for impropriety. The forensic accounting investigator should also consider how the alleged wrongdoing could have been concealed. In essence, if the alleged activity did occur, the forensic accounting investigator should be asking:

- How could it have happened?
- Were system controls overridden?
- How would I hide it in the system?
- What were the controls?
- How did cash get out the door?[14]
- How were accounting records adjusted and balanced?
- How were assets diverted?
- Who would have had to be involved?
- Were third parties such as vendors or customers involved?

It has been our experience that most anonymous tips usually merit further investigation because many contain a kernel of truth. In one case, an anonymous tip pointed to financial reporting issues involving a long-standing financial manager.

[14] A simple technique is to determine how the cash or asset got out the door of the corporation and then work backward to the original source of the funds or the location of the asset.

The forensic accounting investigators immediately focused on internal controls related to check disbursements. After investigating the controls in this area, conducting interviews, and performing data mining, they discovered weaknesses that enabled the suspicious transactions to occur. Among the weaknesses was a practice of presigning blank dual-signature checks, which could then be signed and cashed by the perpetrator. Further investigation revealed that the finance manager had covered up the fraud by faking annual auditors' reports and signing off on them himself. The embezzlement had started many years before and increased in frequency and amounts as the years went by.

In such matters, the forensic accounting investigator will often have to address the question, How can we fill a documentary gap? Proving that a document has been falsified is usually easier than collecting evidence to demonstrate that an omission has been covered up, a document trail has been destroyed, or individuals have colluded. It is typically necessary that forensic accounting investigators piece together information to surround an issue in such a way that even though a specific document has not been found or no one has confessed to wrongdoing, the facts build on each other sufficiently to allow sound conclusions to be drawn.

Consideration also needs to be given to the time period of the impropriety, as suggested by the allegations. If it is alleged that a specific event happened at a single point in time, the issue of time period is less relevant. However, if it is alleged, for example, that an individual has been stealing inventory and falsifying records for an extended period, then consideration must be given, at least in the early stages of an investigation, to the necessity and cost-effectiveness of investigating every incident. In some cases, it may be essential to gain a complete picture of the economic loss in order to make the necessary adjustments to the financial statements. In other circumstances, it may be necessary only to find evidence of one incident rather than every occurrence. For example, if the allegation involves kickbacks from suppliers to the head of purchasing, evidence of one instance may be sufficient to conclude on the matter and take remedial action.

Finally, on one hand, the forensic accounting investigator should approach the allegations with an open mind; no allegation can be dismissed without due investigation. On the other hand, the forensic accounting investigator should avoid the trap of believing allegations without supporting evidence. A common scenario involves allegations founded in truth but embellished or clouded with emotional rhetoric. The forensic accounting investigators may find themselves repeatedly coming back to an allegation, asking the same questions, and determining whether any new pieces of information support or dismiss the allegation. Proving the negative—filling information gaps with sound evidence—can be a very difficult task.

INTERVIEWING EMPLOYEES

Documentary evidence is key to the investigation and establishment of the facts, but the complete story rarely can be established without structured interviews.[15] In light

[15] Consideration must be given to various issues when interviewing employees, including attorney–client privilege, advice to employees, the company's obligations to employees,

of the allegations and an understanding of relevant business processes, the forensic accounting investigator and investigative team need to draw up a list of employees who may be able to provide initial insights on systems, processes, procedures, department structures, and documents.

If it is possible to establish the identity of the source of the anonymous communication or if the individual self-identifies,[16] an early interview will often add key information and enable the investigative team to assess the credibility of the allegations. Whenever possible, the investigative team should conduct its interview after sufficient review of facts and evidence has been performed to test the veracity of the allegations. It will often be necessary and appropriate to reinterview the individual after the accuracy of the information provided has been corroborated.

Identifying the source of the tip may create a dilemma for the investigation team depending on the facts and circumstances. The company should use care in dealing with the individual so as to avoid allegations of harassment and to avoid providing a basis for the individual to allege retaliation. However, the company may need to take action to protect other employees and assets. Furthermore, the individual may have uncovered a serious corporate misdeed and may need to be protected from harassment by other employees. Often, the treatment of the individual in question needs to be managed carefully because the person has key knowledge and occupies a reasonably responsible position in the business, which may suffer commercially without that person on the job.

A decision needs to be taken as to whether to tell employees of the tip, to show them a copy of the tip, or to refer only to the fact that allegations have been made. Once employees become aware of the issues, they will naturally speculate as to who may be the whistle-blower or who would have had access to the information. The interview process, while creating speculation, is essential to the investigation by helping the team determine and evaluate:

- Which individuals (employees, former employees, customers, suppliers, and others) may have the most relevant information about the allegations
- Which additional individuals should be interviewed
- Which documents should be secured and obtained, including e-mail

This relatively open search for truth may generate new lies and could reveal the identity of the whistle-blower. Employees who participated in the improprieties, or others with knowledge of them, may craft stories so as not to expose their participation or knowledge or both, and after the interview they may warn co-conspirators. Interviewing is, therefore, a calculated risk in any investigation.

---

provision of separate counsel, and the potential for an employee to refuse to cooperate. These topics are covered in Chapter 20; the present chapter addresses issues unique to the response to an anonymous letter.

[16] Whistle-blowers often reach out for help by leaving obvious clues to their identity in the hope that the investigators will identify them and make the first approach. When investigators request information, whistle-blowers can experience the lifting of the burden and in some cases the feeling of guilt associated with proactively disclosing the issues.

Concerning possible targets of the investigation, the forensic accounting investigators should consider the personal circumstances of the individual involved—for example, whether the person is in debt, is living in what seems excessive luxury, or is involved with unsavory elements. And the person may also have assets that can be traced back as acquisitions from the proceeds of fraud. The forensic accounting investigators should factor these issues into evaluating the motivation of the individual, the validity of the person's statements, and whether there may be alternative motives. A final point—whether or not the source has been identified—concerns the potential involvement of third parties. For example, is it one person in one department? Is it people across several departments? Is it an external fraud? Or is the perpetrator in collusion with an external party such as a customer or supplier?

On occasion, the forensic accounting investigator may use modified audit procedures to assist in resolving the allegations. In some instances, the forensic accounting investigator may opt to request transaction confirmations from certain suppliers or customers or simply telephone them to verify transactions. One recent investigation involved allegations that salespeople were inflating revenues by billing consigned goods to customers. As part of the receivable confirmation process, the forensic accounting investigators included additional line items such as the amount of consigned goods. When the confirmations were received, it was easy to determine which companies and salespeople to investigate further by taking note of discrepancies in the confirmations related to consigned goods.

In many instances, the anonymous tip may allege kickbacks or phony invoices with a certain supplier or customer. To determine whether the allegation has merit, the forensic accounting investigator may first conduct a public records search to determine the existence and location of a company. Consider these facts from an anonymous tip:

- Operations manager dictates to purchasing department which packaging supplier to use.
- No bids are obtained from other suppliers.
- In the past six months, packaging suppliers that had enjoyed long-term business relationships with the company have been discontinued.
- An employee believes the operations manager is creating the invoices that are being approved by one of his buddies.
- Packaging supplies are being received, but customers are complaining about quality.

Before visiting the premises of the company, forensic accounting investigators determined that the address of the supplier was five minutes from the client company's site and that the company had paid this packaging supplier approximately $500,000 over the past six months. On the way to the client company's site, the forensic accounting investigators drove by the address and took a photograph (Exhibit 8.1). The picture showed an ordinary house in an economically deprived area of the city. There was no signage for a packaging business. The company's legal counsel took the view that this photograph was sufficient predication to continue the investigation, and in time many of the original allegations were confirmed.

The interview process should consider the impact of an investigation on the operations of a business. Because operations must continue, the investigation should

EXHIBIT 8.1 A Revealing Forensic Photograph

be designed to disrupt the business as little as possible—although here, too, there are calculated risks. In situations involving customers and suppliers, the company is often reluctant to approach those parties for fear of damaging ongoing business relationships. Disruption may also occur when individuals are interviewed, and that needs to be considered. The investigative team should weigh the benefits of quickly determining whether there is any basis for the allegations against the potential for some degree of disruption in normal operations.

A common situation in investigations of anonymous tips is the identification of a former employee, perhaps one who had been with the company for some time but who recently departed the area of the company under investigation. This former employee may be the whistle-blower or know the whistle-blower. Employees in this category often provide a wealth of information. For that reason, the forensic accounting investigator should always have an inquiring mind as to who else should be interviewed or may have knowledge of the issue. There may be situations in which knowing the whistle-blower or being reasonably certain of the identity of the whistle-blower can be helpful in evaluating the veracity of the allegations. Identifying such knowledgeable persons early in the process may bring efficiencies to the investigation and can assist the investigative team in focusing on important details easily overlooked if former employees are not considered on the list of possible interviewees.

The forensic accounting investigator and investigative team need to combine the information gained through interviews, public records searches, data mining, hard-copy document review, e-mail review, and electronic discovery to piece the puzzle together. To confirm the facts, they may find it necessary to reinterview individuals several times, comparing their notes with other documentary evidence as well as other interviews. The forensic accounting investigator may have to interview very junior members of a department or organization to identify potential discrepancies in statements gained through interviews.

In this chapter we have only briefly covered issues related to the identification, collection, and control of documents obtained in the course of investigation. Those topics are addressed in detail in Chapter 10. However, a few thoughts may be helpful here. In investigations of the type now under discussion, preserving a record of who provided documents and computer files and precisely when they provided them often is critical to developing sound conclusions. The record makes it possible to compare the responses of an individual (or source of information, if not an employee) over time and evaluate whether there is an indication of that person's involvement or guilt. Depending on the size of the case and the nature and volume of the information, consideration should be given to using an evidence management system. Such systems are often helpful in graphically presenting trails of evidence and relationships. Regardless of the sophistication of the evidence management system, it is necessary to keep strict control of all evidence to maintain integrity and ensure that all available evidence is brought to bear in the investigation.[17]

The majority of the information flow in a modern office is in electronic form; for that reason, it is often necessary to consider evidence in electronic form and to use computer forensic techniques.[18] Electronic discovery can also uncover key documents—for example, a prior draft of a document that was modified to cover up the issues or an e-mail that was deleted by both sender and all recipients. Once identified by the forensic accounting investigators, such documents can be used to confront individuals on the inconsistency of their statements. When a blatantly inconsistent document or statement is identified, individuals will often admit additional facts.

FOLLOW-UP TIP

Just when the forensic accounting investigator has exhausted all areas of inquiry, has reviewed all documentation, has interviewed all relevant individuals, and believes it is time to pack up, sometimes a follow-up tip arrives. Such tips usually follow the same themes as the initial tip, covering the same issues and urging the company to keep looking. Sometimes the relator indicates that the forensic accounting investigators are not on the right path and so provides additional details. A tip of this nature can indicate that the relator is still employed by or has access to current employees of the company. In one case, the relator was identified as a former employee and—given the nature of the matter—the investigative team was concerned that there were active communications between current employees and the relator. After analyzing the phone logs of certain suspected employees, the team identified a clear pattern of communication between an employee and the whistle-blower, his former colleague.[19] Knowing this information helped the team craft its inquiries and interviews and build

[17] If there is the potential for criminal violations, extreme care must be used to document the chain of custody of the evidence and the integrity of the original documents.

[18] Computer forensics and electronic discovery can often provide the critical information in a format that allows for effective data mining. Specific recommendations for how to do this can be found in Chapter 17.

[19] In this case, the employee would call the relator within minutes of completing the interview.

trust with these employees. The team was able in this way to obtain the facts that validated the allegations.

Given that whistle-blowers are typically fearful for their own positions and wish to avoid any reprisal or stigma, every effort should be made to make it simple and safe for them to contact the investigation team discreetly and in confidence. Once an investigation is under way and especially after receipt of a follow-up tip, the investigative team should consider setting up a hotline or central contact. There is value in a tactic as simple as having the investigative team members give out their business cards and in making sure that the corporate grapevine knows where to contact the team during and after business hours. In one investigation, the team members let it be known that they would be staying at a certain hotel for a week. At 11 o'clock one night, the relator called and provided additional details on the issues, including who specifically was involved.

CONCLUSION

Whistle-blower communications are increasingly frequent phenomena. In the wake of corporate scandals, lawmakers are responding to public concern by encouraging employee monitoring of corporate ethics and affording statutory protection for whistle-blowers.

Dealing with an unexpected anonymous tip can be a challenging matter, even to the most seasoned forensic accounting investigator. Objective analysis and the strategic approach taken by professionals skilled in corporate investigations can assist clients in successfully addressing issues that may have serious legal and financial implications. Protection of employees from retaliatory action and the company's need to decide whether or not and to whom to disclose information are among the many issues created by the receipt of an anonymous tip. While the typical initial impulse of the company is to simply hunt down the whistle-blower, the key to resolving cases of anonymous tips usually involves a detailed examination of large amounts of data obtained from many different sources such as interviews, public records searches, data mining, hard-copy document review, and electronic discovery.

A careful, experience-based investigative strategy is imperative to best address the circumstances surrounding the transmittal and receipt of an anonymous tip and to tackle the allegations prudently and thoroughly.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 9

Personal Privacy and Public Disclosure

Hugo Teufel III, Sanjay Subramanian, and Sergio Pedro

INTRODUCTION

With the dawn of the information society, more than at any time in the past, vast amounts of information are available to the forensic accounting investigator to search for and provide context to the information relevant to the investigation. In addition to paper documents, information may be stored on myriad devices, such as laptop and desktop computers, networked servers, personal digital assistants (PDAs), cell phones and smartphones, floppy disks, CDs, DVDs, flash drives, voicemail systems, security logs, video recordings, offsite vendor back-up systems, disaster recovery tapes, and so forth. Often-quoted estimates predict that more than 90 percent of an organization's data may be stored electronically.[1] In fact, many larger organizations have terabytes[2] if not petabytes[3] of electronically stored information (ESI) that could potentially be mined in an investigation during the electronic discovery (or e-discovery) process.[4]

These data often include sensitive information, including personally identifiable information (PII) such as human resource files, home addresses, personal checking and savings accounts, Social Security numbers, and health information. All of this information, whether provided by the employee, held in the company's possession, obtained through an open records request, or purchased from a commercial data reseller, is fodder for the investigator and may also be discoverable in litigation. Indeed, in the United States, the federal Rules of Civil Procedure allows parties in

[1] *The Sedona Principles,* 2nd ed.: "Best Practices, Recommendations and Principles for Addressing Electronic Document Production."
[2] 1,099,511,627,776 bytes, or 1,024 gigabytes.
[3] 1,125,899,906,842,624 bytes, or 1,024 terabytes.
[4] *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery,* published by the Sedona Conference, defines *e-discovery* as "the process of identifying, collecting, filtering, searching, de-duplicating, reviewing and potentially producing ESI that relates to pending or reasonably anticipated litigation in the host or foreign country."

litigation to obtain significant amounts of ESI, including PII, provided that it may lead to information relevant to the dispute and is admissible as evidence in court.

Globally, access to PII is not so easy. Since World War II, in response to the increasing facility of governments and businesses to know the most intimate details of the lives of individuals, there has been a trend toward more rigorous legal protections for the privacy of individuals and their data. Beginning with the United Nations' Universal Declaration of Human Rights in 1948, countries have formally recognized the right to privacy or data protection, limiting the ways in which governments and businesses may use personal information for otherwise legitimate purposes like investigations and marketing.[5] When conducting an investigation, the forensic accounting investigator must be aware of the relevant jurisdiction's privacy or data protection laws and must work closely with counsel to ensure that the company is not exposed to greater risk or liability during the investigation and any related litigation. More importantly, what may be an acceptable investigative technique or required discovery practice in one country may not be so in others.

Concordant with the rise in the protection of personal privacy has been a global movement toward the transparency of public institutions. National and local governments have opened government records and meetings to the public. Of course, given the significance of government to businesses and individuals today, government has vast amounts of information in its records, and it behooves the forensic accounting investigator to make use of this information when relevant to the investigation.

This chapter contains a brief background of the conflicting global data privacy and data processing laws as well as potential ways that an investigator may navigate the challenges arising from these conflicts. This is followed by a discussion of the public open records or disclosure laws in the United States and in other jurisdictions that may help an investigator obtain useful information pertinent to the investigation.

DATA PRIVACY: PROVIDING CONTEXT

At the core of data privacy laws are the Fair Information Practices (FIPs), a globally accepted set of principles for addressing privacy. These are: (1) Notice or Awareness; (2) Choice and Consent; (3) Access and Participation; (4) Integrity and Security; and (5) Enforcement or Redress.[6] Notwithstanding that the core principles are globally accepted, data privacy is viewed differently around the world. It can be a fundamental right, a liberty interest, a social construct, or a combination of the three, depending upon the culture or society. The differences in how people view privacy are, in part, based on how they view government and commerce.

The United States, whose founders distrusted the unchecked power of government, has laws and regulations in place that limit government's access to information and activities within the zone of privacy. Businesses typically have greater flexibility with respect to the use of their employees' and customers' personal information. Privacy rights within the United States generally are statutory, not constitutional, and sector-specific, not omnibus.

[5] Universal Declaration of Human Rights, Article 12 (December 10, 1948).
[6] www.ftc.gov/reports/privacy3/fairinfo.shtm.

European countries, whether within the European Union or not, often view data protection as a fundamental right (in fact as a "human right")[7] and have omnibus laws that limit government and business use of personal information. Data protection commissioners, part of parliament yet independent of the executive branch of government, serve in an oversight and regulatory capacity and may take legal action against those who violate the country's data protection laws. Curiously, in spite of a series of oppressive governments that operated surveillance states (Nazi Germany, East Germany, the Soviet Union, and some others), European data protection laws often are much stricter on business than on government, with significant exceptions for law enforcement, security, and intelligence services. For example, in Europe, as opposed to in the United States, there is widespread use of closed circuit television (CCTV) surveillance coupled with license plate recognition software for use by local and national governments. Also, most European countries have national identification cards in addition to driver's licenses and passports, and most European countries require hotels and guest houses to provide law enforcement with names and other information about overnight guests.

Exhibit 9.1 lists commonly found types of high-risk data that a forensic investigator generally cannot move across international borders without carefully considering whether the appropriate safeguards are in place. Mishandling these data could lead to significant contractual or legal liability, serious damage to an organization's image or reputation or both, or legal, financial, or business losses.

DATA PRIVACY IN THE UNITED STATES

Historically, the Constitution of the United States has provided some privacy protection to individuals, if only as applied against federal and state governments. The Fourth Amendment bars unreasonable searches and seizures without a warrant. Under this amendment, the Supreme Court has recognized the right to privacy in the context of wiretapping or eavesdropping and has required a warrant before listening in on a conversation, provided there is a reasonable expectation of privacy in the conversation.[8]

Over time, however, the Court has subsequently narrowed the right to privacy, assuming that the information (for example, bank or phone records) provided by a third party to the authorities is not covered under the Fourth Amendment because no reasonable expectation of privacy exists, limiting reliance upon the Fourth Amendment as a constitutional source of privacy protection.[9] Beyond the Fourth Amendment, privacy protections are statutory, applicable only against federal and state governments, and often sector-specific. Also, in the United States, data privacy is often focused on PII, such as health records, financial records, Social Security information, and so forth. This is a much more narrow definition than is used in European data protection laws, which may protect e-mails from individuals, even on

[7] EU data protection laws derive from Article 8 of the European Convention on Human Rights of 1950.
[8] *Katz v. United States,* 389 U.S. 347 (1967).
[9] *United States v. Miller,* 425 U.S. 435 (1976); *Smith v. Maryland,* 442 U.S. 735 (1979).

EXHIBIT 9.1 Examples of High-Risk Personal Information

Personally Identifiable Information

- Name and initials in any combination
- Home address
- Home telephone number
- Personal e-mail address
- Personal phone number
- Date of birth
- National identification number
- Driver's or operator's license number
- Credit history
- Mother's maiden name
- Passport number
- Criminal convictions
- Social Security Number (U.S.)

Health/Insurance Information

- Physical or psychological state
- Disease state
- Medical history
- Diagnosis by a health care professional
- Prescription information
- Health insurance identification / account number
- Insurance claim history

Personal Characteristics

- Age
- Gender
- Marital status
- Nationality
- Sexual history or sexual orientation
- Racial or ethnic origin
- Religious beliefs

Financial Data

- Credit, debit, or ATM card numbers
- Bank account numbers
- Other financial account numbers
- Other payment card data (for example, expiration dates, security codes, personal identification numbers (PINs), magnetic stripe data)

Employment Information

- Income
- Salary
- Service fees
- Other compensation
- Background checks

corporate computers, as personal information. European data protection laws focus on the content of the communication, rather than the ownership of the communication device. For example, a personal e-mail sent from a company-owned computer would be discoverable in the United States but could be considered protected under European data protection laws.

Relevant Sector-Specific Privacy Protections

There are a number of sector-specific privacy laws that the investigator may face in the United States. Covering them all is beyond the scope of this chapter and book, but there are three sectors worth noting for the forensic accounting investigator: the federal government; the financial sector; and the health care sector.

The Federal Government The U.S. government began considering the privacy implications of information technology in 1973 with the publication of a report from an advisory committee of the Department of Health, Education, and Welfare (HEW). The HEW advisory committee report made a number of recommendations to include establishing a code of "fair information practices" governing the collection, maintenance, and use of PII by the federal government and establishing an independent

federal agency with responsibility for privacy oversight.[10] Around this time, congressional committees chaired by Representative Otis Pike and Senator Frank Church investigated law enforcement and intelligence agency abuses in conducting domestic surveillance and intelligence gathering on U.S. citizens within the United States.

Congress, informed both by the HEW report and the Pike and Church committee hearings, passed the Privacy Act, which set forth a comprehensive regime limiting the collection, use, and dissemination of personal information held by government agencies. PII covered under the Privacy Act may be shared within an agency based on the need to know, but outside of the agency only if subject to a routine use set forth in a "system of records" notice. Generally speaking, third parties may not obtain Privacy Act–protected PII absent written permission from the person about whom the information pertains. The Privacy Act also established penalties for improper disclosure of personal information and gave individuals the right to gain access to their personal information held by federal agencies. Congress did not include within the Privacy Act authorization for an independent privacy oversight agency.

The Financial Sector Two major laws with privacy provisions that a forensic investigator is likely to come across are the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). GLBA's predecessor, the second Glass-Steagall Act of 1933, was passed in response to the banking collapse during the Great Depression. The second Glass-Steagall Act established the Federal Deposit Insurance Corporation (FDIC) and also prohibited a bank holding company from owning other financial companies such as investment banks and insurance companies. In 1999, Congress passed the GLBA, which repealed part of the Glass-Steagall Act and opened up the financial services market, allowing the mega-mergers between banks, securities firms, and insurance companies that followed.

GLBA also set forth privacy rules that these organizations must follow. Within GLBA, sections 6801 through 6809 stipulate the requirements surrounding the disclosure of nonpublic personal information.[11] The privacy provisions of GLBA conform generally to the fair information practices enunciated in the Privacy Act of 1974. The act limits sharing of nonpublic information with unaffiliated third parties unless the holder of the data can prove that it has complied with the notice requirement.

---

[10] The report listed five principles: (1) There must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for a person to find out what information about the person is in a record and how it is used; (3) there must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent; (4) there must be a way for a person to correct or amend a record of identifiable information about the person; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. A subsequent government commission expanded the fair information practices to eight: the openness principle; the individual access principle; the individual participation principle; the collection limitation principle; the use limitation principle; the disclosure limitation principle; the information management principle; and the accountability principle. From the Privacy Protection Study Commission, *Protecting Privacy in an Information Society* (Government Printing Office, 1977).

[11] www.ftc.gov/privacy/glbact/glbsub1.htm.

This requirement specifies that the holder of the data must provide an opt-out capability to the consumer, who may then register the desire to not have that data shared with unaffiliated third parties. Financial institutions, as well, must provide an initial privacy notice to the consumer at the time of establishing a business relationship and not less than annually during the continuation of such relationship. Financial institutions may share information with affiliated companies and service providers.

The Fair Credit Reporting Act—Beginning in the 1940s, businesses shared customer information to make consumer access to credit easier. By the 1960s, consumers found that they were impeded by inaccurate credit information that credit reporting agencies had about them. Individuals often had no means of seeing what information credit reporting agencies had on them, let alone the right to seek redress for inaccurate or incomplete information.

In 1970, Congress passed the Fair Credit Reporting Act (FCRA), the first federal law to limit business use of PII to cover consumer reports used, in whole or in part, for establishing a customer's eligibility for credit, insurance, employment, or other business purpose. Consumer reports are defined broadly to include information pertaining to creditworthiness, character, general reputation, or personal characteristics. Organizations that compile consumer reports and persons who use consumer reports are covered under the FCRA. The Act requires accurate, current, and complete third-party data when used for decision making; consumer notice when third-party data are used to make decisions affecting them; access to consumer reports and redress for consumers when reports contain errors; and the use of consumer reports only for lawful purposes. Civil and criminal penalties apply for violations of the FCRA, which may be enforced by the Federal Trade Commission, state attorneys general, or consumers.

The Health Care Sector *The Health Insurance Portability and Accountability Act*—In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), in part to protect insurance coverage of workers and their families when changing jobs. HIPAA and the regulations issued also established privacy and security requirements for the transmission or use of protected health information (PHI) in whatever form. Directly covered under HIPAA and the HIPAA privacy and security rules, promulgated by the Department of Health and Human Services (HHS), are covered entities, such as health care providers, health plans, and health care clearinghouses. "Business associates" were covered indirectly through their contracts with covered entities.[12] Importantly, covered entities may not use or disclose PHI, except as provided under the privacy and security rules. HHS and state attorneys general may enforce HIPAA, and failure to comply could result in civil and criminal penalties, with fines of up to $250,000 and ten years of imprisonment. HIPAA, as well, does not preempt state laws that provide greater protection.

In 2009, Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA).[13] Title XIII of the Act made significant changes to HIPAA. Known as the

[12] *Business associates,* generally speaking, are entities that perform activities involving PHI on behalf of covered entities. Law and accounting firms, web hosting providers, and even investigators may be considered business associates under HIPAA.
[13] Pub. L. No. 111–5 (2009).

Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of the ARRA extended aspects of HIPAA and the regulations, established breach notification requirements for covered entities and business associates, limited some uses and disclosures of PHI, and increased enforcement and penalties for the privacy and security provisions. Significantly, the HITECH Act extended coverage of the security rule to business associates directly. Forensic investigators involved in health care investigations should exercise caution when handling PHI to ensure that they do not violate restrictions in the use of that information.

Breach Notification

The downside of information technology and the ability to amass and manipulate large quantities of data, including personal data, is that sometimes there are breaches of data. The law has caught up to the on-the-ground reality of data incidents and breaches. More than 40 U.S. states and territories have breach notification or disclosure laws that require companies to notify consumers when their data were inadvertently disclosed to a third party. Breaches have often been the result of disclosures from third parties who had access to the data and did not protect them. The forensic investigator with PII from even a few dozen individuals may be covered by breach notification laws from one or more states. If that information is PHI, the investigator may be covered by the HITECH Act, discussed earlier. An investigator who is responsible for a breach of PII may find that not only does she have to notify affected individuals and to remediate the possible damage, but that the investigation is compromised because it has been made public as a result of the notification.

Electronic Discovery

As a common law country, the U.S. legal system is an adversarial system that expects both sides in a litigation to obtain, preserve, and share relevant information. Under Rule 26(f) of the United States federal Rules of Civil Procedure, parties are required to "meet and confer" before the commencement of the trial on the relevant sources and types of ESI that may be required in the discovery process.[14] As such, companies must be careful to preserve all relevant accessible data, whether it supports their case or hurts it.

Generally, if data are "reasonably accessible," an entity in the United States may be required to produce the data so long as they are nonprivileged. If the requesting party finds it necessary and provides "good cause," nonreasonably accessible data may be required. What is considered "nonreasonably accessible" can be debated, but, in general, any back-up or legacy tape that is "unorganized, incapable of search functions or otherwise unintelligible" falls into this category.[15]

---

[14] www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

[15] Gavin Foggo, Suzanne Grosso, Brett Harrison, and Jose Victor Rodriguez-Barrera, "Comparing E-Discovery in the United States, Canada, the United Kingdom, and Mexico," www.mcmillan.ca/Upload/Publication/BHarrison_ComparingE-Discoveryintheunitedstates.pdf. Web publication, October 13, 2009.

In the United States, a company faces a substantial risk of sanctions due to the intended or unintended destruction of relevant data because of decisions like the landmark *Zubulake v. UBS Warburg* case. In this case, the judge instructed the jury to infer negatively that e-mail not preserved by UBS was purposely not retained, because it might have damaged UBS's case. As a result, UBS was fined $29 million in punitive and compensatory damages.[16] Such case law in the United States places the issue of e-discovery on an equal footing with compliance with national and state data privacy statutes.

DATA PRIVACY IN THE EUROPEAN UNION

Introduction

The European Union's privacy laws stem from the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950. Article 8 articulates "the right to respect for private and family life."[17] The article states, "Everyone has the right to respect for his private and family life, his home and his correspondence." In the 1970s, the law was adjusted to extend the right to privacy of data on private and public sector databases.

As business shifted to a more global scale, the need for laws governing cross-border transfers became necessary. In 1981, the Council of Europe crafted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and the Organisation for Economic Co-operation and Development (OECD) issued its Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Both documents had, at their core, variations of the fair information practices.[18] In late 1995, the European Union's Data Protection Directive (95/46/EC) was published.[19] Laying the foundation for the Data Protection Directive are the Fair Information Practices. This directive states, "in accordance with this Directive, member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." This directive prohibits data from being transferred outside of the Union unless adequate protection of privacy exists in the outside country.[20] All EU member states must have data protection laws at least as strict as the EU Data Protection Directive.

---

[16] Gregg L. Weiner, "E-Discovery: It's Getting Scary Out There: Trying to Triumph in a World Most Lawyers Don't Understand," *American Bar Association* 14(4) (March/April 2005).

[17] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, open for signature November 4, 1950, entry into force September 3, 1950.

[18] To compare with the U.S. statement of the fair information practices, the OECD version is as follows: the collection limitation principle; the data quality principle; the purpose specification principle; the use limitation principle; the security safeguards principle; the openness principle; the individual participation principle; and the accountability principle.

[19] Directive 95/46/EC of the European Parliament and of the Council, October 24, 1995.

[20] M. James Daley and Kenneth N. Rashbaum, eds., *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery,* The Sedona Conference, August 2008; www.thesedonaconference.org/dltForm?did=WG6_Cross_Border. Web publication, October 13, 2009.

The European Union has provided guidance on how best to comply with data privacy laws in the form of directives. Directive 95/46/EC, Article 26, explicitly states that all data that are attached and traceable to a particular individual are covered by the European Union's data privacy laws. That is, the source of the data is not relevant; rather, merely the extent of anonymity determines whether or not data are protected. It is important for the investigator to understand the specific terms referred to in EU law. A *data subject* is a natural person, identifiable, directly or indirectly, by the personal data. Status as a data subject is not dependent upon nationality, but upon location. Non-Europeans whose data are collected or used in Europe are covered under European data protection laws. A *data controller* is the person who decides the purpose and manner in which data are to be processed. A *data processor* is the person who carries out the data processing instructions of the data controller. *Processing* is what is done with the data, to include collection, recording, storing, organization, transmission, blocking, or destruction.[21]

The directive suggests taking all avenues available to determine the identity of the owner of data so as to determine the extent of anonymity. So, data may be stored on a network server and not locally on any particular individual's computer; it is still possible, however, for the data to have some affiliation with the individual and therefore be covered by the European Union's data privacy laws.[22] Most countries in the European Union have legal systems based on civil law. The civil law system is statutorily based, as opposed to the adversarial nature of common law. Civil law countries tend to lack formal discovery procedures, as one would find in the United States. These nations are consequently less concerned with collecting and preserving "personal property" and more concerned with protecting it. Under the 1995 EU Data Protection Directive, any information that relates to a specific individual is considered personal property. Even more personal is sensitive data that reveal an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sex life.[23] Businesses holding sensitive data must apply additional protections.

The bottom line is that internal investigations and discovery in U.S. federal court cases are far more complex when personal data in Europe is involved. In the United States, standard procedure would be to collect all potentially relevant data from company files and servers, whether paper-based or electronic. Investigators would image workstations, laptops, and handheld devices and pull back-up tapes. Under EU data protection laws, however, an investigator could run afoul of the law by collecting all potentially relevant data without consideration of pertinent data protection issues. Companies and investigators, generally speaking, may not use personal data for purposes other than those that were the basis for the collection of the data. Monitoring of employee e-mail may be limited, with personal e-mails and folders off limits to the investigator. Implementation of ethics hotlines for anonymous whistle-blowers to report fraudulent activity and other Sarbanes-Oxley (SOX)–compliant activity are difficult, at best. Litigation is no different. From the parties' perspectives, as well

---

[21] Directive 95/46/EC of the European Parliament and of the Council, October 24, 1995.
[22] European Union. European Parliament. Luxembourg. EUR-Lex. October 24, 1995. http://eur-lex.europa.eu/en/index.htm. Web publication, October 14, 2009.
[23] EU Data Protection Directive Art. 8, ¶ 1.

as the federal Rules of Civil Procedure, the priority in the United States is often to preserve and collect ESI or risk claims of spoliation, while in Europe, countries are more concerned with protecting personal data, regardless of what it might contain.[24]

Three examples of the data privacy laws in Europe are detailed as follows:

France

France's privacy laws are more restrictive than the average European Union member state. France's Commission Nationale de l'Informatique et des Libertés (CNIL), an independent administrative authority protecting privacy and personal data, provides guidance regarding compliance with data protection obligations. Violation of French data protection laws can carry both civil and criminal penalties and will likely result in reversals of adverse actions against employees and conflict between U.S. and EU laws.[25]

In France, firing an employee after reading that employee's e-mails in an investigation into whether the employee was engaged in freelance work on company time, contrary to company policy, may result in civil liability. In *Nikon France v. Onos,* an employee successfully sued his former employer for having fired him for working on freelance matters on company time at the office.[26] The company had discovered his moonlighting activities while reading e-mail of his marked "personal." In 2005, McDonald's sought to implement a SOX-compliant ethics hotline that would have permitted employees to anonymously report instances of fraud. The CNIL disapproved of the plan, because of concerns for managers' data protection rights.

With respect to e-discovery, France's "blocking statute," which builds upon the EU's data privacy laws, is a 1980 law[27] prohibiting the disclosure of "information or documents that are of economical, commercial, industrial, financial or technical nature to a foreign authority in the course of civil or administrative proceedings unless this disclosure complies with applicable laws and treaties."[28] French authorities likely would consider the blocking statutes to apply to the transfer of information from a French subsidiary to a U.S. parent. Judges must navigate a specific process before they can obtain evidence from an entity in France. First, the judge must have the information recipient forward a request to the French Minister of Justice, who then forwards the request to a "competent judge." This judge may then determine if the request has sufficient relevance to the legal proceedings and whether the request specifically identifies which documents the recipient wants.[29]

---

[24] Foggo.
[25] French Act No. 78–17 of January 6, 1978, on Data Processing, Data Files, and Individual Liberties, Article 51 (amended by the Actove August 6 2004, relating to the protection of individuals with regard to the processing of personal data).
[26] Cass. Soc., Arrêt No. 41–64 (Oct. 2, 2001).
[27] Section 1134 of the civil code, section 111–4 of the criminal code, 1bis of the law n° 68–678 dated July 26, 1968, amended by the law n° 80–538 dated July 16, 1980.
[28] Lisa Nuch Venbrux, *Privacy and Security Law* (Arlington, VA: The Bureau of National Affairs, 2009).
[29] Ibid.

Germany

Germany is a federal republic. The 16 laender, or state, governments each have data protection commissioners. There is a federal data protection commissioner as well. German data protection laws are among the strictest in the world.

The world's first data protection law was passed in the German laender of Hesse in 1970, followed by a Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG) in 1977. Data protection received a significant boost in 1983, when the German Federal Constitutional Court recognized an individual's "right of informational self-determination." This right is limited only by the "predominant public interest."[30] More recently, Germany amended the BDSG to align with the EU Data Protection Directive. The BDSG covers transfers of PII abroad, surveillance, anonymization, smart cards, and sensitive data collection. All automated data processing must be registered with the federal data protection commissioner.

Internal investigations in Germany are limited both by a variety of data protection laws and company works councils. The Telecommunications Act of 2004 establishes privacy for electronic communications. Companies permitting employee use of the Internet at work for private use are, in effect, providers of telecommunications services, subject to the Act and the works councils, should the company wish to conduct surveillance. If the company expressly prohibits private use of the Internet at work, the general data protection law applies and, consistent with the Fair Information Practices, the employer must limit monitoring to the absolute minimum, based on a solid suspicion of an individual employee, because surveillance is necessary to assess an employee's performance.

Germany is typical of a civil law country that has no formal discovery process. As detailed in the European Union's Article 29 Working Party document on pretrial discovery in Germany, "litigants are not required to disclose documents to the other party; instead a party needs to only produce those documents that will support its case."[31] The opposing party must move the court for production of additional documents. The motion must be specific describing the document and it must include facts demonstrating what the document would prove and justifying production of the document. Therefore, unlike in the United States, there is no compelling reason for a party to hand over a "smoking gun" document to an opposing party, especially if the opposing party is unaware of the existence of that document.

Also, Germany is the first European country to implement a data breach notification law, amending the BDSG. Data controllers must notify data subjects and data protection authorities whenever a breach threatens significant harm to the data subject.[32] For larger breaches, notification may be made through publication of half-page notices in at least two national newspapers.

---

[30] Federal Constitutional Court (*Bundesverfassungsgericht*) decision of December 15, 1983), ref. no. 1 BvR 209, 269, 362, 420, 440, 484/83 (cited in *Privacy and Human Rights,* at 480–481).

[31] Working Document 1/2009 on pretrial discovery for cross-border civil litigation, Article 20, Data Protection Working Party, February 11, 2009.

[32] BDSG Section 42a.

The United Kingdom

Privacy laws in the United Kingdom build upon the laws of the European Union. The U.K. Information Commissioner's Office is the independent body charged with overseeing privacy and freedom of information.

Although part of the European Union, the United Kingdom is a common law state, so it differs from civil law member states like France and Germany. In a common law country, an entity is required to disclose all relevant documents, whether those documents support or weaken its case.[33] The fair information practice of proportionality is fundamental to what data must be produced in the United Kingdom. The requesting party can demand specific documents, but the court will consider the importance of the documents, financial well-being of the company, the amount in dispute, and the difficulty of obtaining the documents before granting discovery. In general, acceptable documents are active, fall within a specific period of time, and have been identified by keyword searches.[34]

NAVIGATING THE LEGAL DIFFERENCES BETWEEN THE UNITED STATES AND THE EUROPEAN UNION

The conflicting codes and statutes from various countries have created a maze through which an investigator must navigate artfully. Businesses concerned with fraud have been punished for failing to adhere to EU data protection laws during the course of internal investigations. U.S. courts have been unsympathetic to restrictions on discovery requests from EU states as well, and EU member states have been equally unconcerned with U.S. requests for discovery. The following two examples demonstrate the increasing risk that businesses may face when subpoenaed to produce data to other countries. One of the first cases involving the complications of conflicting laws in cross-border e-discovery was *Strauss v. Credit Lyonnais,* from 2007. A U.S. judge ordered a French company, Credit Lyonnais, to produce documents to the court; in doing so, Credit Lyonnais violated French data privacy laws and the company's lawyer was fined €10,000. In 2008, UNAT Direct, the British arm of American International Group (AIG), was fined €640,000 for producing documents outside Britain for e-discovery. These two examples illustrate the difficulties that companies are experiencing in responding to cross-border e-discovery subpoenas.[35]

Before undergoing an internal investigation, the investigator must work closely with U.S. and local counsel to assure that the investigation or discovery procedures comply with all relevant laws. The investigator should document the actions taken as well, both to establish the thoroughness of the investigation and to confirm that the collection has been undertaken in good faith.

The following are some considerations for the investigator and company when dealing with U.S. and EU cross-border investigations and discovery.

---

[33] Daley.
[34] Foggo.
[35] Brandon Cook, "Why Cross-Border Litigation Is a Compliance Concern," *Sarbanes-Oxley Compliance Journal* (2009), April 7, 2009, http://www.s-ox.com/dsp_getNewsDetails.cfm?CID=2599. Web publication, October 14, 2009.

Works Councils and Whistle-Blowers

Throughout the European Union, a company with at least 1,000 employees within the member states and at least 150 employees in at least two member states has an obligation to inform or consult its works council with respect to a company's use of employee personal data.[36] Works councils are separate from labor unions and are recognized in EU law.[37] Whether the law requires notice or consultation varies. In France, the Labor Code requires informing and consulting works councils on activities that lead to control of employee activities.[38] In Germany, as a leading practice, even if not required by local law, a business should consider notifying the works council of its intent to use personal data for an investigation. An additional leading practice is to finalize agreements with works councils in advance of the handling of investigations and electronic discovery. Finally, if a company is considering instituting an ethics hotline, it should consider the Article 29 Working Party's opinion on whistle-blowing programs.[39]

Cross-Border Data Transfers

Standard Contractual Clauses One avenue at an investigator's disposal for obtaining and analyzing data from countries with conflicting privacy laws is to employ standard contractual clauses (SCCs). Under Directive 95/46/EC, corporations that seek to move information outside the European Union must "ensure 'adequate protection' for personal data."[40] In an attempt to clarify the obligations that these multinational organizations have in complying with the EU directive, the European Union has created and approved several sets of SCCs that provide "a legal basis for data transfers from" the European Union.[41] An SCC is a *voluntary,* yet legally enforceable declaration in which the data exporter and data importer agree to process said data compliant with basic data protection rules.

The first instance of these model clauses was introduced in 2001. They initially covered only controller-to-controller transfers and later expanded in scope to include controller-to-processor transfers as well.[42] Their primary purpose is to provide for

---

[36] Directive (94/45/EC).
[37] Ibid.
[38] Art. L432–2–1.
[39] Article 29 Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistle-Blowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.
[40] "Data Protection: Commission Approves Standard Contractual Clauses for Data Transfers to Non-EU Countries," June 18, 2001; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/851&format=PDF&aged=1&language=EN&guiLanguage=en.Web publication, October 13, 2009.
[41] Christopher Kuner, "The E.U. Alternative Standard Contractual Clauses for International Data Transfers" (Arlington, VA: Bureau of National Affairs, 2005), http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1002%5CEU_Alternative_Standard_Contractual_Clauses_ kuner_ 2.05.pdf. Web publication, October 13, 2009.
[42] Kuner.

corporations a "straightforward means of complying with their obligation" to protect personal data that are to be transmitted outside the European Union.[43]

Safe Harbor Another avenue at the United States's disposal for preventing inadvertent loss or disclosure of data is the voluntary Safe Harbor process, which is intended to facilitate U.S. compliance with EU Directive 95/46/EC. Safe Harbor is a process that was established between the U.S. Department of Commerce and the European Commission to allow for the transfer of data between Europe and the United States while maintaining the data protection principles expected within the European Union.[44] A key benefit of Safe Harbor is that the transfer of data can occur without the approval of a Data Protection Authority (DPA). As with all transfers of data from Europe, an investigator should seek the advice of the client's internal counsel as well as competent external counsel, especially if the data are considered personal sensitive data, such as health, racial, and sexual orientation information.

The European Commission recognizes United States companies that abide by the Safe Harbor Privacy Principles (issued by the United States Department of Commerce) as offering comparable protection. As such, SCCs are not necessary for data transfer to the United States, in the event that the United States entity adheres to the Safe Harbor principles.[45] However, if the transfer includes information not protected under Safe Harbor, a standard contractual clause can provide the necessary privacy measures.[46] Because these clauses list specific obligations for the data exporter, data importer, and other third parties, they are a practical measure for companies that simplify "compl[iance] with [the] obligation to ensure 'adequate protection' for personal data transferred to the rest of the world."[47]

Binding Corporate Rules An investigator may also consider binding corporate rules (BCRs) as another means of obtaining and analyzing data from foreign sources.

At a high level, BCRs are a set of intracorporate privacy policies used to transfer personal data from one nation to another. Corporations may use BCRs after receiving approval from a DPA.[48] A key limitation for an investigator is that while a BCR allows for the cross-border transfer of PII within a corporation, it does not provide authorization for onward transfer for litigation without additional safeguards.[49]

---

[43] "Data Protection: Commission Approves Standard Contractual Clauses for Data Transfers to Non-EU Countries," June 18, 2001; http://www.out-law.com/page-1731. Web publication, October 13, 2009.
[44] www.export.gov/safeharbor/eg_main_018236.asp.
[45] Data Protection.
[46] European Union, European Commission, Internal Market, "Companies helped to fulfill data protection rules," *Single Market News,* June 2002; http://ec.europa.eu/internal_market/smn/smn29/s29mn35. htm. Web publication, October 13, 2009.
[47] Data Protection.
[48] *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery*. A Project of the Sedona Conference on International Electronic Information Management, Discovery, and Disclosure (WG6).
[49] *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery*. A Project of

The Hague Convention Another mechanism commonly invoked for formally obtaining evidence in another country is the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters.[50] This treaty is used to obtain evidence from witnesses in other nations that are also signatories of the convention. At the time of publication, 48 nations, including many European countries, are parties to the Hague Evidence Convention.[51] While this convention plays a key role in the sharing of evidence internationally, its scope is limited in two ways: The data in question must be used as legal evidence or "to perform some other judicial act," and both nations must be members of the convention.[52]

Other Options Examples of additional ways a U.S.-based investigator could request and process EU-based data include:

Receiving consent from the individuals related to the PII. This consent must be informed, unambiguous, freely given, specific in nature, and given before the transfer.[53]

Leveraging the work of a local subsidiary or third party. The entity performing the work could be based in the EU country in question, within another EU member state, or within a country whose data protection regime is deemed adequate by the EU (for example, Switzerland).

Having the company or a third party anonymize the data, for example, by replacing names with unique identifiers known only to the company or third party. It is recommended that the entity that is anonymizing the data be based in the EU country in which the data are located, within another EU member state, or within a country whose data protection regime is deemed adequate by the European Union. This way, the sensitive data never leave the EU country in question, and only the cleansed data are sent to the United States.

Regardless of the option used, it is strongly recommended that an investigator consult counsel with experience in cross-border data transfer laws and regulations before proceeding with an investigation. In many countries, the content of a message—rather than the equipment on which it was composed—determines whether the message can be classified as a personal and private matter.

ELSEWHERE AROUND THE GLOBE

Countries outside of the United States and the European Union have varying levels of data privacy that may also limit the discovery scope for an investigator. For example, in Canada, an entity must disclose any document that has been possessed

---

the Sedona Conference on International Electronic Information Management, Discovery, and Disclosure (WG6).

[50] www.hcch.net/index_en.php?act=conventions.text&cid=82.

[51] www.hcch.net/index_en.php?act=conventions.authorities&cid=82.

[52] www.hcch.net/index_en.php?act=conventions.text&cid=82.

[53] *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery.* A Project of the Sedona Conference on International Electronic Information Management, Discovery, and Disclosure (WG6).

or controlled by, or in the power of, someone related to the litigation. The term *document,* in addition to paper documents, includes all data and information that are in electronic form. Entities must reference provincial guidelines for how to store and produce electronic data.[54] In the United States, "any back-up tapes containing the documents of a key player must be preserved and accessible." These documents include e-mail and other electronic files.[55] Similar to United States law, Canada requires the preservation of electronic data.[56] While the United States has a practice direction requiring one to search for deleted and residual data, however, no such guidance exists for Canada.[57]

Latin America

Latin America trends toward the European approach, with many countries having constitutional provisions that provide for individuals to seek legal recourse to obtain information in the possession of others about themselves and to have the information corrected or destroyed, as appropriate.[58] After many years of military dictatorships and other authoritarian governments, these new democracies tried to provide additional protections to their citizens, one of which was *habeas data,* or, the right to "have the data."[59] Although it is implemented slightly differently in each country, in general, it protects the individual's image, privacy, honor, information self-determination, and freedom of information.

Although most existing data protection laws in Latin America are based on the European Data Protection Directive, there are important distinctions among the countries. Argentina is currently the only Latin American country recognized as adequate by the European Union (that is, it meets EU data protection standards), but Uruguay's steps have brought them closer toward achieving EU certification.[60] Uruguay's law 18–331 uses the EU "adequate level of protection" guidelines when ensuring data protection in transferring personal data internationally.[61] Brazil, the first country to implement habeas data, has limited privacy protections. The Brazilian constitution provides for access to and correction of personal data in the possession of the government but not its update or destruction.[62] It is permissible as well, under Brazilian law, for an employer to monitor employee use of e-mail on

[54] Daley.
[55] *Treppel v. Biovail Corp.*, 249 F.R.D. 111
[56] Foggo.
[57] Daley.
[58] Andres Guadamuz, "Habeas Data: The Latin American Response to Data Protection," *Journal of Information, Law and Technology,* 2000.
[59] Andres Guadamuz, "Habeas Data: The Latin American Response to Data Protection," *Journal of Information, Law and Technology,* 2000.
[60] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/932&=HTML&aged=0&language=EN&guiLanguage=en.
[61] Wim Nauwelaerts, "Uruguay Close to Receiving EU Adequacy Recognition?" Hogan and Hartson, *Chronicle of Data Protection,* October 2, 2009; http://www.hldataprotection.com/2009/10/articles/international-compliance-inclu/uruguay-close-to-receiving-eu-adequacy-recognition/. Web publication January 8, 2010.
[62] Constitution of the Federal Republic of Brazil (1988). Article 5, Section LXXI.

company-owned computers.[63] Also, in Argentina, Uruguay, and Peru, legal entities are considered within the scope of the data protection laws; in Chile, the laws protect only individuals. Chile and Argentina regulate both public and private sector uses of personal information, but Peru's laws pertain only to private stores of information. Finally, Mexico is considering implementation of an EU-style data protection law.

Asia Pacific

The Asia Pacific approach to privacy is outlined in the Asia Pacific Economic Cooperation Privacy Framework.[64] Based on the Fair Information Practices, the APEC privacy framework promotes a consistent approach to information privacy protection as a means for ensuring the free flow of information in the Asia Pacific region.[65] The objectives of the APEC privacy framework are to develop appropriate privacy protections for personal information; prevent the creation of unnecessary barriers to information flow; enable multinational businesses to implement consistent approaches for the collection, use, and processing of data; and promote domestic and international efforts to enforce information privacy protections.[66] The APEC framework applies to the personal information of living individuals, although publicly available information is excluded. It also applies to persons or organizations that collect, hold, or process personal information.

In Japan, data privacy in the private sector is regulated primarily under the Personal Information Protection Act (Law No. 57 of 2003). This Act defines personal information very broadly: "Information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)."[67] When a business receives personal information, it must disclose to the subject (or publicly) the purpose of use. Generally, this Act prohibits "unconsented transfers of personal data to third parties, with the exception of certain outsourcing companies (for example, payroll processing)."[68]

South Korea has adopted an Act on Promotion of Information and Communications Network Utilization and Data Protection of 2001 (ADP), modeled after Germany's Online Service Data Protection Act of 1997, which "allows the data subject to withdraw consent for the collection, use and disclosure of data at any

---

[63] Tribunal Superior do Trabalho, 1ªTurma, Relator: João Oreste Dalazen, RR–613/2000–013–10– 00, DJ–10/06/2005.

[64] APEC Privacy Framework, 16th APEC Ministerial Meeting, Santiago, Chile, November 17–18, 2004.

[65] The nine Fair Information Practices of the APEC framework are: preventing harm, notice, collection limitation, use of personal information, choice, integrity of personal information, security safeguards, access, and correction and accountability.

[66] www.apec.org/apec/news_____media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

[67] Personal Information Protection Act (Law No. 57 of 2003), Article 2, Paragraph 1, www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

[68] Thomas Shaw, "E-Discovery in Asia/Pacific: U.S. Litigation Exposure for Asian Companies," *The Privacy Advisor* 9(11): December 2009.

time and requires the data user to comply unless the preservation of such personal information is required by another Act. Further, every data subject has a right to access and correct his or her personal information."[69] There have been multiple unsuccessful attempts to merge the public and private sector provisions into a unified data protection system with an independent regulatory body.[70]

Also, China has recently considered passing an amendment to their legislation, which would heighten data protection provisions on personal information. This would criminalize the misappropriation of data not only by government personnel but also in several private sectors (for example, financial, telecommunications, transportation, educational, and medical institutions).[71]

PUBLIC DISCLOSURE

In contrast to privacy and data protection laws (which limit the access to and use of personally identifiable information), disclosure laws are about the public availability of information in the possession of government agencies. In the United States, this information is often available through the federal Freedom of Information Act (FOIA) or other federal laws. Whatever the means, an investigator can uncover much information about relevant issues, individuals, and organizations from government agencies, even directly from government web sites.

The Freedom of Information Act

At the federal level is the U.S. Freedom of Information Act (FOIA), enacted in 1966. It is one in a series of laws, starting with the Administrative Procedure Act (APA),[72] intended to provide greater transparency to the American public. Congress has amended FOIA many times since 1966, limiting exemptions and broadening coverage of electronic records. Importantly for forensic accounting investigators and others, federal agency records are presumed to be publicly available, absent coverage under one of nine exemptions or three law enforcement exclusions described a little further on. Moreover, many of the nine exemptions are considered discretionary, not mandatory. An informed requestor, working with agency FOIA officials, can develop significant information on subjects of interest.

What follows is a highlight of aspects of FOIA relevant to the forensic investigator. For additional information, the reader is encouraged to visit the U.S. Department of Justice's web site, which has the Department of Justice's Guide to the Freedom of Information Act (2009 FOIA Guide). The FOIA Guide details the available information, how to submit a request, the appeals process, and other relevant information regarding the Act.[73]

---

[69] www.privacyinternational.org/survey/phr2003/countries/southkorea.htm.
[70] Graham Greenleaf, "Twenty-One Years of Asia-Pacific Data Protection," *Privacy Laws and Business International Newsletter* 100: August 2009; Web publication, January 8, 2010.
[71] www.hunton.com/files/tbl_s10News/FileUpload44/15919/china_personal_information_1.09.pdf.
[72] 5 U.S.C. § 1002.
[73] www.usdoj.gov/oip/foia_guide09.htm.

An investigator seeking to use FOIA must understand that it is a federal law and does not apply to state or local governments, nor does it apply to the private sector. Additionally, it only covers executive branch agency records, not legislative or judicial records. To constitute an agency record, the agency must have created or obtained it, and be in control of the record at the time of the request.

Once the investigator has made the decision to seek agency records in aid of an investigation, the investigator should give thought to the agencies that may have relevant information. Sometimes, another agency may have the same information, collected for that agency's mission. What may be exempt from disclosure at one agency may be subject to discretionary disclosure at another agency, or be a public record.

Generally, anyone may make a FOIA request for any reason, and an investigator or counsel is not required to identify the client when seeking records from the government. There are only three classes of requesters whose requests will not be fulfilled: fugitive felons; requests from any foreign government or international governmental organization, either directly or indirectly, to agencies of the intelligence community; and persons who have waived their FOIA rights by plea agreements are precluded from making FOIA requests on the subject of the waiver.[74]

FOIA requires requests with reasonable specificity. Uncertainty over the scope of the request may delay an agency's response or result in a "no records" determination. If uncertain about the type of records requested, the investigator may be able to work with the agency's FOIA office to narrow the scope of the request. FOIA also requires a written request (e-mail is acceptable) to the proper office within the agency. Once received, time begins running for the agency to respond, which is typically 20 days. If uncertain, the investigator may submit a request to the main FOIA office within the agency, likely delaying the response time. Again, contacting the FOIA office to help with pinpointing the components within the agency likely to have responsive records may be advisable.

Before making a request, an investigator should be familiar with the agency's FOIA regulations (usually found on the agency's web site) for it to have a better understanding of the agency's FOIA structure and procedures. Depending upon the nature of the request, some records may be found in the FOIA reading room or elsewhere on the agency's web site. Finally, the requester must be prepared to pay. Agencies are likely to view investigators as falling under the "commercial use" requester category and not within the educational institution, noncommercial scientific institution, or news media representative categories. Therefore, investigators are often responsible for paying the costs of searching for, reviewing, and copying responsive records. It is advisable to list in the written request a dollar amount below which the investigator is willing to pay without further consultation. At the time of publication, standard amounts vary from $50 to $250.

FOIA Exemptions Federal agencies are required to release records, provided that they do not fall under one of nine exemptions, or three law enforcement exclusions. Not all exemptions are mandatory, and agencies can—and should—consider discretionary disclosure when in the interest of the public to do so. While an internal corporate investigation may not be in the public interest, making certain records available to

[74] 2009 FOIA Guide, at 42–43.

the public information of interest to the investigator may be. The investigator won't know until he asks.

Exemption 1 protects information that is classified in the interests of national defense or foreign policy.[75]

Exemption 2 covers internal personnel rules and practices of an agency.[76]

Exemption 3 covers information statutorily exempt from disclosure, an example of which is the Privacy Act of 1974.[77]

Exemption 4 covers trade secrets and commercial or financial information obtained from a person that is privileged or confidential.[78] This exemption is significant for businesses because its intent is to encourage the sharing of information with government, which information is truthful. The investigator should be cognizant that information provided to the government during the course of the investigation may itself be subject to disclosure under FOIA. Depending upon what the investigator provided, there may be grounds for a reverse FOIA action against the government, in which a person or organization sues the agency to keep information from being released.

Exemption 5 of the FOIA covers inter- and intra-agency records that would not be available by law to a party other than an agency in litigation with another agency.[79] This exemption covers records that would be exempt from disclosure in civil litigation, such as attorney–client privileged communications, attorney work product, and records that fall under the deliberative process privilege.

Exemption 6 covers personnel, medical, and similar records whose disclosure would constitute a clearly unwarranted invasion of personal privacy.[80] This exemption is separate from the coverage of the Privacy Act of 1974. If an investigator seeks records that pertain to an individual or that contain personally identifiable information, the investigator should consider whether it is feasible to get a written waiver from the individual to avoid a denial under the Privacy Act of 1974 or Exemption 6 of the FOIA. Exemption 6 is another of the FOIA exemptions in which reverse FOIA litigation has occurred.

Exemption 7 covers records or information compiled for civil or criminal law enforcement purposes, with some limitations (for example, release would interfere with an investigation or deprive a person of the right to a fair trial, or could reasonably be expected to constitute an unwarranted invasion of privacy).[81]

Exemption 8 covers matters that are "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions."[82] This exemption is intended to ensure the security of financial institutions and to safeguard the relationship between banks and supervising agencies.[83]

---

[75] 5 U.S.C. § 552(b)(1).
[76] 5 U.S.C. § 552(b)(2).
[77] 5 U.S.C. § 552(b)(3).
[78] 5 U.S.C. § 552(b)(4).
[79] 5 U.S.C. § 552(b)(5).
[80] 5 U.S.C. § 552(b)(6).
[81] 5 U.S.C. § 552(b)(7).
[82] 5 U.S.C. § 552(b)(8).
[83] 2009 FOIA Guide, at 661.

Exemption 9 covers "geological and geophysical information and data, including maps, concerning wells."[84] This exemption is intended to prevent unfair competitive harm to speculators and parties negotiating over the use of wells.

There are three exclusions to FOIA that can prevent the disclosure of information: (1) ongoing criminal investigations that are not publicly known, (2) the threatened identification of confidential informants in criminal proceedings, and (3) certain intelligence-related records of the Federal Bureau of Investigation.

An agency response to a FOIA request will either grant or deny the request in whole or in part, or state that no responsive records exist. If the investigator is dissatisfied with the response, there are two options. First, the investigator may want to work informally with the responding FOIA office, especially if the response is a "no records" determination. Second, the investigator may submit an appeal. As with the initial request, the agency has a time limit in which to respond. Failure to respond within the time limit may be deemed a denial of the appeal, which will allow the investigator to seek judicial review. An investigator submitting an appeal should work with counsel and should list as many bases as possible for the appeal, including a request for a discretionary release if any asserted exemptions by the agency are not mandatory. If, after receiving a decision on appeal, the investigator is still dissatisfied, judicial review is available.

Other U.S. Federal Governmental Agency Information

Whether under the FOIA, the APA, or another federal law, there is a wealth of information potentially relevant to the forensic accounting investigator through the federal government. The Equal Employment Opportunity Commission (www.eeoc.gov), the Federal Trade Commission (www.ftc.gov), the National Labor Relations Board (www.nlrb.gov), the Occupational Safety and Health Administration (www.osha.gov), and the Environmental Protection Agency (www.epa.gov) have much information on their web sites relating to consumer, labor, and environmental issues and sanctions. Also:

The U.S. Department of Defense (DOD) (www.defenselink.mil) has records on service members past and present.

The National Archives and Records Administration maintains records of inactive military personnel and naturalized citizens (www.archives.gov).

The U.S. Bureau of Prisons (www.bop.gov) maintains records on individuals who have been incarcerated in federal prisons.

The Securities and Exchange Commission (www.sec.gov) provides access to quarterly, annual, and other reports filed by publicly owned companies, as well as the adjudication of any disciplinary matters related to individuals or public entities.

Some commercial databases, such as LIVEDGAR (www.dsionline.com) and 10-K Wizard (www.10kwizard.com), allow searches of thousands of SEC filings, through which the forensic accounting investigator may be able to establish an association between the subject of an investigation and companies or transactions previously unnoticed.

---

[84] 5 U.S.C. § 552(b)(9).

The Occupational Safety and Health Administration (www.osha.gov) lists workers' compensation claims and other information.

The Federal Election Commission (www.fec.gov) records contributions to federal election committees, political parties, and political action committees.

U.S. State Disclosure Laws

All 50 states and the District of Columbia have freedom of information laws. Whether based on FOIA or the Model Open Records Act, state freedom of information laws are sometimes applied less stringently than their federal counterpart. The public interest against disclosure often prevails during the administrative process and even in judicial review. The investigator is advised to work with local counsel if seeking records from state or local agencies.

Notwithstanding, an investigator may be able to glean substantial information from state agencies and their web sites. For example, records from each state's prison are available online (www.corrections.com/links/viewlink.asp.?Cat=30). Also, state gaming commissions maintain records of the owners of gaming establishments, the financial information of gaming establishments, and the names of individuals banned from gaming establishments. For example, the Nevada Gaming Commission's Excluded Person List maybe found at http://gaming.nv.gov/loep_main.html.

International Disclosure Laws

Personal privacy and public disclosure are linked, in that privacy is strengthened through transparency of government operations. Unfortunately, there is no automatic correlation between a country's privacy or data protection laws and its open records laws. Moreover, information available in the United States is not always available in foreign countries, and vice versa. More than 80 countries have enacted freedom of information laws, with legislation pending in several more countries. With the exception of Sweden, which passed the first freedom of information law in 1766,[85] most freedom of information laws globally are relatively recent and untested, with weaker disclosure provisions. For example, the United Kingdom's Freedom of Information Act (FoI) was passed in 2000 with an exemption for information that would prejudice the public interest.[86] The public interest exception has been construed broadly. In 2004 and 2005, an American journalist made a series of requests for the expense records of members of Parliament (MP), which Parliament rejected. This request, if made in the United States of senior government officials, would be granted routinely. After a series of hearings, administrative and judicial, the journalist and others who had joined the process prevailed, but not before unredacted copies were leaked to the media. The expense reports showed that a number of MPs from the majority and minority parties had received taxpayer reimbursement for personal expenses. There were unsuccessful calls to amend the FoI Act to exclude MPs and Parliament from its coverage and some MPs lost their seats.

[85] Freedom of the Press Act of 1766.
[86] Freedom of Information Act, 2000.

CONCLUSION

An investigator working with multinational clients must have a strong understanding of the legal requirements surrounding data privacy and protection in each of the countries in which the clients operate. As much as possible, the investigator should work proactively with knowledgeable counsel to understand the possibilities and limitations to conducting investigations and gathering and producing ESI for discovery purposes in each of these countries so that they are able to quickly react to the demands of a new investigation. Informed consent, safe harbor, standard contractual clauses, binding corporate rules, the use of local in-country resources, and the anonymizing of data are all ways to potentially mitigate the U.S.–EU cross-border investigation dilemmas.

An investigator should also know that while legislation as well as data privacy and protection statutes might limit the sources of data available for discovery, increasing public transparency rules such as the Freedom of Information Act in the United States may allow for a wealth of previously inaccessible information for data-mining purposes. Again, it is best to work with local counsel who is experienced with the country's disclosure laws when seeking information.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 10

Building a Case: Gathering and Documenting Evidence

Frederic R. Miller and David L. Marston

Gathering, documenting, and retaining evidence are crucial steps in any investigation and critical to forensic accounting investigations. Decisions taken with respect to the gathering of evidence are intertwined with judgments about the scope and manner of investigation, and the value of the conclusions of an investigation ultimately rests on the credibility of the evidence discovered. Thus, care must be taken at all times to properly gather, preserve, store, and use evidentiary materials. Performed correctly, the means and manner of evidence gathering create a clear, straightforward, and convincing trail to the ultimate conclusions of the investigation. Conversely, laxity or error in the handling of evidentiary material may obscure the logic of an investigation and undercut its conclusions.

One should always begin an investigation as if the matter may end up in a criminal court, and for this reason take all appropriate steps to gather and preserve the evidence. Even if it is believed at the outset that it is unlikely the matter will be referred for prosecution, it is best to maintain that option. After all, one never knows where investigations may lead, and there may be no choice in the matter if an enforcement agency decides that the investigation is of interest.

In forensic accounting investigations, several types of evidence are normally relevant, and most of them are documentary in nature. Documents generally can be divided into broad categories: those that exist in electronic form or media and those that are physical in nature, such as paper documents. The two categories often overlap in that a document available in electronic form may have been printed and perhaps modified by notations placed on it by a recipient. Another type of evidence commonly encountered, indeed often critical to the success of forensic accounting investigations, is testimonial evidence of people who were involved in the matter. This generally takes the form of oral explanations offered to the investigative team and is reflective of either people's memory of events or their interpretation of documents containing information about the events under investigation. Gathering such evidence presents issues that differ from the collection of either electronic or physical documentary evidence.

Finally, in addition to business records created contemporaneously with the issues, transactions, or matters under investigation, the forensic accounting

investigators themselves may create documents that ultimately become evidence of the scope and findings of the investigation. Those documents may be presented as evidence to regulators, arbitrators, or courts charged with adjudicating or regulating the matters under investigation. Like the business records of the company, these materials must also be the subjects of proper preservation and control.

CRITICAL STEPS IN GATHERING EVIDENCE

Considerations at the Time of Retention

While each investigation has unique requirements, in most cases the proper gathering and preserving of evidence call for similar considerations and steps. Those considerations begin at the outset of the engagement by consideration of the conditions under which the forensic accounting team has been engaged and the setting forth of basic expectations about the handling of evidentiary material in the engagement letter. The two key points at this stage are: (1) Will any portion of the evidence be subject to privilege—either the attorney work product privilege or the attorney–client privilege? (2) Who will be responsible for preserving the evidence and for how long?

Whether any evidence gathered or created in the course of an investigation is subject to privilege is a legal issue that cannot often be predicted with certainty. If you are retained by in-house counsel or outside counsel, your work product may, in fact, be privileged, and as such it is best to treat all work product as though it were privileged. If, down the road, the client wishes to assert privilege through its counsel, you will at least have done everything in your power not to have waived the privilege in the course of your work. The expectation of privilege is often set out in the forensic accounting investigators' retention letter. If the privilege is contemplated, prudent practice makes make clear in the letter that (1) counsel will direct and supervise the forensic accounting investigators' work and (2) materials created for analyzing or summarizing the findings of the investigation are executed at the direction of counsel for counsel's use in giving legal advice to the client. And there is a third key point: Have both counsel and the client sign the retention letter.

To the extent it is contemplated that the privilege will apply, among other things, the forensic accounting team members should not disclose information to others who have no role in the engagement, should not discuss the matter with client personnel without the permission of counsel, and should formalize their expectation that the material is privileged by recording an appropriate legend on each document at the time of its creation. Thus, for example, an analysis of an accounting issue in the form of a schedule should bear the legend *Privileged and Confidential: Attorney Work Product* or *Privileged and Confidential: Prepared at Counsel's Request in Contemplation of Litigation,* as appropriate. Because analyses are prepared throughout an investigation, they change as new information is discovered or old information is understood in a new light. In response to the circumstance, it is customary practice also to use a legend such as *Draft: Subject to Change* on the work product, as appropriate. Forensic investigators should consult with counsel regarding these and other practices that should be followed to protect privileged communications.

Document Retention Considerations

Document retention and preservation are especially significant in forensic accounting investigations of financial statement issues. This is a complex area and should be discussed with counsel, but following are some considerations.

In the ordinary course of business, transactions are executed; divisions are acquired or sold; accounting systems are modified, updated, or replaced; and estimates are changed as new information becomes available. All of those things may be relevant to preserving the electronic evidence resident in a corporate accounting system. At the beginning of the engagement, it may be appropriate to consider whether the forensic accounting investigator will be responsible for retaining records as the records exist at a given date—for the benefit of the company and the investigation team—and, if so, exactly what documents and for how long the documents should be retained. Document retention practices represent a complex area, and counsel should be consulted in this regard to ensure compliance with firm policies and all applicable laws and regulations. There are usually massive amounts of paper and computer files that get created or reviewed during the course of an investigation, and it may be burdensome to retain every document and electronic file. However, there may be situations in which that may be exactly what is required under the circumstances. One such situation would be when subpoenas call for such information.

In some matters, the forensic accounting investigator may be asked to review evidence collected pursuant to grand jury proceedings. Such evidence is confidential and may be shared only with those who have signed the required confidentiality statement pursuant to Rule 6(e) of the Federal Rules of Criminal Procedure, commonly referred to as a *6(e) statement*. The obligations undertaken in the 6(e) statement are personal, and the forensic accounting investigators should be aware that it is a crime to disclose federal grand jury materials to unauthorized parties. Separate filing and other document-handling procedures within the office may need to be established so that only those authorized to view the material have access to it.

Planning Considerations

Depending on the issue under investigation, it is often necessary to meet with the client to discuss the types of evidence you may require and to locate that evidence for the time periods under review. This is especially true of financial accounting records, owing to the constantly changing business structure of many entities and of those entities' data processing operations. If, for example, you plan to perform an e-mail review of six people at the company for the past two years, you may be sadly disappointed when you show up with your information technology (IT) and investigative staff at company headquarters, only to learn that offsite backup tapes cannot be located and the e-mail server rewrites over files every 60 days. It is best to plan for these issues ahead of time. Such planning considerations should include the following:

- Review of client's record-retention policies and whether there is compliance
- Storage locations for paper records, both on- and offsite
- Imaging technology used for transaction documents, such as customer invoices, vendor invoices, and contracts

- Existence and storage of employee files
- Existence of files at employees' homes, including home computers
- File retention practices at different corporate locations, which may vary substantially
- Organizational chart and reporting hierarchy
- Storage medium for computerized records, both on- and offsite
- Backup procedures used for employee computers and e-mail, including when backups occur and what information is lost or retained and what is contained on servers versus individual hard drives
- Retention of records kept by or about former employees of the company
- System changes in relation to corporate accounting systems or e-mail systems
- Existence of documents related to outsourced corporate functions such as payroll and internal audit

Creation of a written plan for the collection of documents is frequently an excellent tool for focusing the efforts of the investigation team on material most likely to be relevant. At the end of the investigation, this plan will serve to show that the scope of investigation in regard to documents sought was appropriate for the issue at hand. This methodical approach also helps avoid the scorched-earth approach that results in the accumulation of an excessively broad collection of records or of different types of records at different locations from different witnesses. In some circumstances, the forensic accounting investigator may legitimately take this approach but should consider a more focused approach at the outset.

Creating a written plan also helps reduce the confusion of terminology that often arises with accounting and financial records. Most forensic accounting investigators have had the experience of receiving documents or materials that fail to fulfill the requirements of a detailed and carefully planned request. The undiscovered fraudster may be behind certain difficulties that come up—for example, conflicting terminology or nomenclature intended to confuse forensic accounting investigators. In one instance, a request for a customary accounting document, an "aged trial balance of accounts receivable," resulted in the surprising response that no such document existed. In fact, the company personnel kept such a record, but it was called the "listing of open receivables." Later, when the facts became known as to who the likely culpable party was, that individual told the forensic accounting investigators that he had not deliberately withheld the document; he simply had not recognized the term used by the forensic accounting investigators. Obtaining a listing of all user reports—identifying the exact report name, users' names, and when the reports are prepared and distributed—often will help avoid this potential conflict. It is also possible that some parties from whom documents are sought may be motivated to deflect the requests by their own legal positions or other concerns. Having a clearly spelled out plan and well-worded requests helps make it possible to expose such behavior in later proceedings.

Creating a Chain of Custody

The chain of custody has the purpose of establishing from the time the evidence is collected to the time of its presentation to a court or perhaps to a regulatory body that it has been properly preserved from alteration or damage and thus retains its

probative value. Before gathering any evidence, the forensic accounting investigator should consider with counsel and the client the level of detailed record keeping necessary to establish the chain of custody over the evidence. For the most part, establishing the chain of custody is merely a record-keeping procedure not very different from physical inventory procedures with which many accountants are familiar. The procedure is used for establishing where the evidence came from and that it has been properly secured since it was acquired, principally against alteration.

Consider the forensic investigation of an inventory theft disguised by the falsification of physical inventory records by a company executive. It may be important to demonstrate what records the executive was aware of and perhaps had under direct control. In this circumstance, creating a record that indicates the location in the executive's office from which each file was gathered will be important. Files taken from the executive's locked desk drawer for which only the executive has the key may be properly viewed in a different light from records taken from a stack on the conference table in the executive's office used for team meetings on a daily basis. Because the different levels of precision require different amounts of time and effort to create and maintain, the establishment of such procedures at the beginning of the evidence-gathering effort is an important cost and efficiency issue. Generally, the more care required to document the chain of custody, the higher the cost to your client for the investigation. For this reason, it is important to agree at the outset of the engagement on the measures that your client requires on this issue and to incorporate the client's instructions in the retention letter, if at all possible.

Creating a written record that identifies the item of evidence, tells where it was found, shows its quantity (for example, the number of pages in a document), and assigns it a control number is an important procedure in establishing the chain of custody. Almost all evidence physically collected by forensic accounting investigators is in the form of documents rather than other physical evidence such as a fingerprint. Properly numbered through a process often referred to as *Bates numbering*[1] and detailed as to their nature and source, copies of documents can generally be made and used during the analytical phase of the investigation. This approach preserves the originals and secures them from loss, damage, or alteration. If that cannot be done and the evidence must be transferred between geographic locations or team members, the written custody record should be updated to reflect the date and time of transfer. The signature of both the delivering and the receiving parties will confirm that each item was in fact transferred. If material is packed in boxes, each box should also bear a unique identifying number and should be tracked through each step in the

[1] The Bates Company was long the source of a mechanical ink-pad number stamp that advanced a counter to the next digit each time the stamp was used. This process became known as Bates numbering, and the numbers themselves were referred to as the Bates numbers of a document. The numbers provide a convenient method for identifying documents exchanged in litigation or collected in an investigation. The process serves to eliminate confusion over which document is being referred to, especially in situations in which the same or similar documents may have been collected from different sources, such as the same memorandum from several different people. Today, many alternatives to the Bates stamp are available, ranging from copy machines to software programs that add numbers to documents.

EXHIBIT 10.1 Photograph Documenting the Condition of Evidence

exchange. Each piece of evidence must be coded such that its location of discovery by the forensic accounting investigator can be determined.

The condition of the evidence should be noted and documented as it is gathered. With respect to documentary evidence, it is important to be alert to indications that the documents may not be complete or authentic. Erasures, use of correction fluid, incomplete printing, and missing pages or attachments may all be red flags alerting the forensic accounting investigators to alterations. Noting such issues at the time the documents are collected creates a record that may be useful later in establishing that the documents were not altered nor sections lost subsequent to their collection. One of the means of recording the collection of physical evidence or of securing devices containing electronic files is to use evidence bags. Although clear-plastic evidence bags are not recommended for most document collections, for notes or other records found in the desks of suspect employees they may be useful.

On global assignments or in situations in which documents are identified and transferred from remote locations, consider augmenting the chain of custody procedures with photographs. The pictures shown in Exhibits 10.1 and 10.2 were parts

EXHIBIT 10.2 Evidentiary Materials en Route

of an investigation in a developing country. The first photograph, sent by e-mail, quickly demonstrated to counsel why some documents were illegible and could not be transported.

Later, when evidence that could be transported was ready for shipment, a photograph of the materials en route supplemented the written chain-of-custody records, consisting of the document and box log, air freight bills, and signatures of receipt once delivered.

In today's world, much of the information pertinent to an investigation may be stored electronically. The following devices often contain relevant data:

- Personal computers
- Network servers
- Wireless and cordless telephones
- PDAs and smartphones
- Answering machines
- Paging devices
- Caller ID devices
- Digital cameras
- Facsimile machines
- Printers
- Scanners
- ID card printers
- Copiers
- Compact disc duplicators
- Smart cards/magnetic stripe cards
- Security systems
- Global positioning systems
- Electronic game devices
- Vehicle computer devices
- Storage media

The best practices for gathering electronic information are constantly changing as technology evolves, and staying up to date requires expert help. The investigative team must have access to the specific IT skills needed to identify and gather all relevant information—and particularly to be able to assess and affirm the integrity of the electronic data. The practitioners who gather and identify the information may differ from the professionals who read and analyze the results. For this reason, make sure that the information gathered during the electronic search includes the make, model, and type of computer(s); internal and external disk drive capacity; operating systems used; applications used; design of the network; and the computer literacy of the users. All of these points would be carefully noted by forensic technologists.

As with documentary evidence, handling electronic evidence requires establishment of a chain of custody. The information contained on the subject computer is considered evidence and must be handled and stored in a manner that ensures the integrity of the data. That is accomplished in a number of ways: by keeping documentation on all procedures and applications performed on the electronic evidence, by storing the electronic media in a secure location (a locked file cabinet or safe), by making a bit-by-bit image copy of the hard drive rather than a file system copy, by

analyzing the copy rather than the original, and by using forensic software to prove the integrity of the original contents.

WHOSE EVIDENCE IS IT?

In gathering both physical and electronic documents, the investigative team may encounter privacy or other issues limiting its right of access to the data and its right to transport data across geographic borders. For example, in collecting desk files or computer files from employees, documents of an obviously personal nature, such as bank account records, may be encountered. In general, personal material should obviously be viewed as outside the scope of investigation and set aside until counsel's advice can be sought as to the appropriate disposition. The laws of foreign countries also vary considerably with respect to privacy and may set limits on both the collection and transportation of data across borders. It may be improper to collect or transport to other jurisdictions employment data such as home address or national identity numbers such as Social Security numbers. Some countries—as a basis for permitting transport of data—have laws that look to whether the receiving nation's laws offer privacy protections equal to their own. For example, some countries, notably Switzerland, have special laws related to banking data. The Swiss bank secrecy laws make it illegal to transport bank account data or documents out of the country.

One significant and far-reaching example of privacy legislation is the Data Protection Act (DPA) enacted by the European Union. The DPA provides that anyone processing personal data must comply with DPA principles. The principles provide that data must be:

- Processed fairly and lawfully
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant, and not excessive
- Accurate
- Not kept for longer than necessary
- Processed in line with the subject's rights
- Secure
- Not transferred to countries without adequate protection

Corporate ownership of data and files related to employees' personal information, or documents created by employees—e-mail, for example—may be protected by one or more privacy regulations. HIPAA[2] regulations in the United States offer an example of such privacy regulations. The forensic accounting investigator should be generally familiar with such regulations, which provide, among other things, that

[2] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires any entity that maintains health records for others (such as its employees) to keep such records private. HIPAA has forced many companies, especially hospitals and HMOs, to overhaul their records storage and retrieval systems and information security standards and policies.

under no circumstances should you avail yourself of medical information of any kind. Where you must be especially careful is in requesting personnel files: Always ask the employer to remove any medical information before giving you a file. As a general rule, it is prudent to obtain clearance from counsel before attempting to gather any such evidence.

EVIDENCE CREATED BY THE FORENSIC ACCOUNTING INVESTIGATOR

Working Papers

During the course of an investigation, the forensic accounting team is more than likely to produce analyses and summaries of the factual material discovered. Such analyses and summaries are likely to form the basis of testimony if litigation to recover losses is commenced, if litigation is brought against the enterprise as in shareholder class-action lawsuits, or if you are instructed or compelled by law to produce them for regulatory or other authorities. Accordingly, care should be taken to include all appropriate materials in the files of the engagement. The practice of cross-referencing analyses to sources of information is critically important and often conveniently accomplished by noting the Bates number of the document from which the data were taken subject to the document retention requirements set forth earlier. The unique subject matter of each investigation will dictate what should be maintained in the working papers, but some types of documents that would typically be included in addition to the report of findings, are the following.

- *Accounting records and other documents.* General ledger, subledgers, financial management reports, reconciliations, journal entries, internal audit reports, purchase orders, vendor information, accounting journals, management reports, contracts, telephone, computer system and security system records, desk files, e-mail files, web sites—and still other types of records and documents in this category.
- *Public record searches.* Reports from third-party investigations, such as related-party evidence, Dun and Bradstreet reports, and investigative reports and information from Internet sites (see Chapter 15): The information may be as varied as newspaper articles, chat room discussions, links to hobbies, and philanthropic and other outside interests and investments. Sources of this material may include filings with the U.S. Securities and Exchange Commission (SEC), accessed through EDGAR.[3]

[3] EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others required by law to file forms with the U.S. Securities and Exchange Commission. Use of EDGAR serves to benefit investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the commission.

- *Electronic computer files.* E-mail (copies of To, From, cc, and bcc), computer files or imaged records of entire drives (see Chapter 17), and data stored in handheld personal digital assistants.
- Photographs or digital photos, preferably with a date and time stamp.
- Chain-of-custody documentation.
- *Interview notes and audio recordings.* Interview notes taken by you and your staff professionals during the investigation of witnesses—both targets and company personnel.
- *Third-party information.* Provided by legal counsel or other interested third parties, this material might include external audit reports, management letters and reports, records of nonaudit services, bank statements (canceled checks, bank advices, and other supporting documentation), and documents obtained by subpoena or search warrants.
- *Court pleadings and deposition transcripts.*

Reports

Providing written reports is not invariably required in investigations. Adding substantial time and cost, written reports may or may not be needed, depending on circumstances (see Chapter 18). As a general practice, retaining evidence and analyses as if a report will be prepared and issued is an appropriate efficiency measure, although the decision as to whether or not that will actually occur can usually be deferred until late in the investigation. In some cases, it is true that you will be informed at the outset of the investigation that a report is required. For example, if conducting a 10A investigation, you may be asked to provide a report for the counsel who retained you to assist in performing the investigation.

The topic of reports is well covered in Chapter 18, but we do wish to address one important issue here. If a report is undertaken, the question arises as to the treatment and distribution of report drafts. The question of drafts may also pertain to analyses or summaries created in the course of the investigation. On these matters, the forensic accounting investigator should have a clearly stated policy (see the discussion on document retention considerations earlier in this chapter) with which all staff are familiar. Counsel should be consulted as to counsel's obligation to retain and produce drafts of reports.

Your firm or company will no doubt have policies and practices regarding what to do if you receive or reasonably anticipate receiving a subpoena for materials collected or created in the course of an investigation or if you reasonably anticipate litigation regarding the subject matter of the investigation. Such policies may cover the handling of all documents, files, notes, and records of any type—even if not considered to be officially part of the working papers—with regard to their preservation and retention.

You should consult your firm or company counsel and your client's counsel, as well, immediately upon the receipt of a subpoena. These consultations provide both sets of attorneys the opportunity to evaluate any means of quashing the subpoena if they conclude that it is desirable to do so and will also permit counsel an opportunity to advise on any document retention issues arising as a result of the subpoena. A forensic accounting investigator retained as an expert witness in a state court matter was once served just after giving a deposition. The subpoena was later quashed

because the party was not permitted by law to subpoena an out-of-state expert witness. The subpoena could still be served in the expert's state of residence, but in this case it was not. The point is, do not assume. Consult with your client's counsel.

WHAT EVIDENCE SHOULD BE GATHERED?

As noted earlier, no hard-and-fast rules exist as to the selection of documents for retention (subject to document retention requirements set forth earlier). The following discussions highlight the types of documents that should be retained in a variety of investigations.

Investigations of Vendors

Investigations of vendors should focus on where the money went and for what purpose. All relevant disbursement information should be collected. That would normally include:

- Vendor information setup in the company's master file data for the accounts payable system
- Contracts, purchase orders, invoices, and documents used to accumulate payment approvals, receiving documents, correspondence concerning credits, billing errors, or other matters
- Internal reviews of vendor quality and the results of public record searches performed to qualify the vendor

Collection of these materials is likely to be facilitated by computer forensic techniques such as data mining for duplicate addresses, similar names, or duplicate payments, invoices, or purchase orders, among other queries. Interviews may be required, as will additional public records searches about the vendors' current situations.

Investigations of Foreign Corrupt Practices Act Violations

Investigations of Foreign Corrupt Practices Act violations typically require disbursement review and interviewing. In one illustrative case, certain large payments related to the award of government contracts were made through a middleman identified in the company's record keeping as a consultant. The investigation team sought to identify the services rendered but could find no fair value exchange for the payment. As in investigations of vendor fraud, thorough payment documentation should be gathered, and interviews focused on the purpose of each payment may be needed. See Chapter 26 for more information.

Investigations of Improper Related-Party Activity

Investigations of improper related-party activity usually require all information regarding the nature of the relationship, interview notes, relevant internal control policies, e-mail streams, and public record searches, as well as any documents that

would support analysis of economic exchange at fair value in an arm's-length transaction.

Investigations of Employee Misappropriations

Investigations of employee misappropriations most often center on the documents and records kept by the employee and may include desk files, computer files, e-mails, records of access to and use of corporate computer systems, records of access to company facilities, security camera tapes, employment records, payroll records, and material obtained in interviews with co-workers. Outside information related to lifestyle and property ownership may also be relevant. PDAs, smartphones, and cell phones in particular should not be overlooked, because they may contain information about people assisting the employee in the scheme.

Investigations of Specific Allegations

Investigations of specific allegations vary widely, arising from whistle-blower letters, hotlines, anonymous tips, and exit interviews. Depending on the nature of the allegations, the investigative team must develop an appropriate plan for accumulating evidence most likely to be relevant. As a general rule, your evidence-gathering plan should begin broadly. Even though some of the allegations could be unfounded or overblown by disgruntled employees, it may be unwise to ignore them. The breadth of the initial response helps demonstrate to any interested third parties such as regulators or external auditors that the allegations were taken seriously and addressed in a complete manner. This degree of thoroughness is a key element in sustaining the conclusions of the investigative team.

Investigations of Financial Statement Errors

Investigations of financial statement errors are likely to require access to just about every element of a company's financial accounting and business records, as well as the files of many employees and the e-mail files of all involved in the subject transactions. Such investigations may also require interviews and the collection of transaction evidence from outside parties such as banks, customers, vendors, and former employees. In major investigations, it may be worthwhile to copy the general ledger system and e-mail servers to another data center location, so that when the investigation team is ready to review the material, the material has been properly preserved.

IMPORTANT CONSIDERATIONS REGARDING DOCUMENTS AND WORKING PAPERS

- Originals should be marked as evidence and filed separately. Obtain permission to remove original documents from a client site.
- Advise staff that most of the working papers are essentially copies of documents and electronic spreadsheets gathered as part of the investigation and that have tick marks, notes, and other descriptors written on them to document your

work. Consider that working papers may need to be produced to a third party. As such, separate copies should be maintained apart from the working papers so that the original document can be replicated or copied as it existed before it was written on as part of the normal course of testing by the forensic accounting investigator.

- Whenever responding to a request by a third party for some or all of your working papers, make a completely separate copy of the documents you send, and create an index of those documents—to be maintained in a separate binder or box. In this way, you will always know exactly what you have given to a third party. Do not simply place a sticky note on a document that reads, "Sent copy to SEC Enforcement." Counsel should be consulted and may even manage this production process.
- Each working paper should stand on its own. You should be able to understand just how the document (working paper) supports a report or findings. This is usually indicated by the tick marks indicating where a particular number may be coming from, that is, its source from another working paper, and where it is going to, that is, its use on another working paper. Tick marks should be explained in a legend proximate to the working paper being reviewed (see Exhibit 10.3). If the purpose or source of the working paper is not clear, then a note written on the working paper should provide such clarity. It is important that each working paper stand on its own so that it can be viewed in the larger context that clarifies its significance.
- Working-paper binders should flow from the report, all the way down to the lowest form of support (see Exhibit 10.4). This means that a clear road map from summary results and conclusions through all summarizations and calculations down to the most detailed item should be included. Such an approach permits a quick and easy determination of how each part of the evidence was used, how each data element was included, or why data elements were not included in calculations.
- There is no requirement that working papers must be neat, but they should be readable and organized. If you are at a restaurant and you write down some important information or do an analysis on a napkin while at lunch, that can become a working paper. If it is readable and understandable, simply tape it to a sheet of paper when you return to your office, and file it in your working-paper binder. Your clients will appreciate your efficiency.
- While reviewing a working paper, if you find a deficiency that can be corrected or clarified with the stroke of a pen, do it then and there. There is no requirement to correct it on your computer and then reprint and refile. If it is possible to be efficient without sacrificing quality or understanding, do it.
- Most investigations are document intensive, and even the simplest of engagements can generate a mass of working papers. Consider preparing a binder that can be used for client meetings when you present updates on the investigation. The binder contains the report or a listing of findings to date, cross-referenced to a tabular index of relevant support (but not all the support). Documents in the binder are just enough of a reminder to indicate to your client exactly what document supports your findings. For example, if a specific contract provision is an important point of reference, include only the first page to identify the contract and to identify the page with the key provision. The balance of

XYZ COMPANY
Summary of Accounts Receivable Write-Offs by Quarter
Q4 Fiscal 2000 - Q3 Fiscal 2001

		Q4 00		Q1 01		Q2 01		Q3 01		Subtotal Q4 00 - Q3 01		
Income Statement Impact												
Acquisition Expense	1.1	$30,000,001	2.1	$1,000,000	3.1	$26,647,535	4.1	$ -	5.1	$57,647,551	✔✔	
Bad Debt Expense		-		-		-		13,411,931		13,411,931		
Miscellaneous Expense		56,931		68,050		116,457		177,025		418,462		
Total Income Statement Impact		30,056,932		1,068,050		26,763,992		13,588,956		71,477,930		A
Balance Sheet Impact												
Accrued Liabilities	1.2	3,339,867	2.2	2,375,414	3.2	6,466,414	4.2	3,451,862	5.2	15,633,572		
Acquisition Accrual		-		-		16,930,463		-		16,930,463		
Allowance for Doubtful Accounts		2,302,580		570,097		1,131,206		2,891,325		6,895,208		
Miscellaneous Other		-		24,339		2,680		956,741		983,761		
Total Balance Sheet Impact		5,642,447		2,969,850		24,530,764		7,299,928		40,442,989		B
Total A/R Write-Offs		$35,699,379		$4,037,900		$51,294,756		$20,888,884		$111,920,919		C
		✔		✔		✔		✔		✔		

Draft - Subject to Change

Attorney Work Product
Privileged & Confidential

Legend:

✔ Foot
✔✔ Cross foot
1.1 - 5.2 Source Document Reference

A+B=C

Prepared by: Edna Everage
Date: 12/31/01

fn: XYZ_Q3_2001

EXHIBIT 10.3 Working Paper with Tick Marks

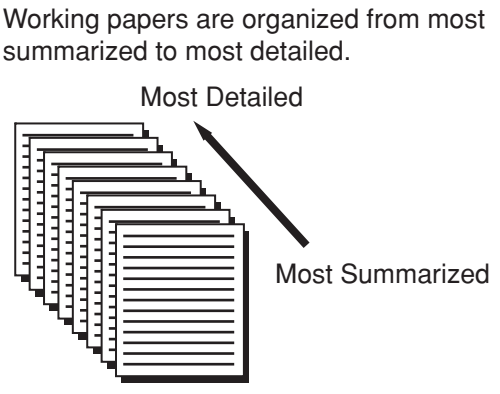


EXHIBIT 10.4 Working-Paper Organization

the longer document can be produced at a later time; it is filed in the complete set of working papers maintained by your staff.

- At the end of an engagement, take time to organize your working papers before sending them to storage consistent with your firm or company's document retention policies.

CONCLUSION

Gathering evidence and keeping proper control of it from the time it is first collected until its ultimate use in legal proceedings or other forms of reporting are highly significant aspects of a properly conducted forensic accounting investigation. Rigorously controlled evidence gathering is the infrastructure on which the credibility of the evidence rests and, consequently, the credibility of conclusions resulting from the investigation. Like all inventory control systems, keeping appropriate records of the chain of custody requires consistency and discipline. Ideally, evidence created by the work of the forensic accounting team should be properly filed, indexed, and controlled.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 11

Independence, Objectivity, Skepticism

Steven L. Skalak and Thomas W. Golden

This chapter divides at the center. On this side of the divide is a necessary account of legislation, codes, and rules that now govern the critical issues of auditor independence, objectivity, and professional skepticism. On the other side are case studies illustrating independence, objectivity, and professional skepticism in action during the course of forensic accounting investigations.

The wave of financial scandals at major corporations in the early 2000s prompted lawmakers to pass new laws governing the accounting industry and the public companies they audit. Sarbanes-Oxley was enacted in part to remedy the perceived weaknesses in corporate governance and oversight of the auditing profession and to eliminate potential conflicts of interest. Among the areas that the Act addresses is auditor independence. In the wake of the recent financial crisis, independence as long practiced by the auditing profession is now being recognized as a responsibility of other capital market participants. For example, the Accountability and Transparency in Rating Agencies Act of 2009 proposed in the United States and the European Union's Regulation of the European Parliament and of the Council on Credit Rating Agencies enacted in 2009 focus on the following four points:[1]

1. First, to ensure that credit rating agencies avoid conflicts of interest in the rating process or at least manage them adequately
2. Second, to improve the quality of the methodologies used by credit rating agencies and the quality of ratings
3. Third, to increase transparency by setting disclosure obligations for credit rating agencies
4. Fourth, to ensure an efficient registration and surveillance framework

It is useful that formal recognition of the responsibility of other capital market participants to act with independence and objectivity is being recognized.

[1] www.house.gov/apps/list/speech/financialsvcs_dem/credit_rating_agencies_draft.pdf and http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=197610.

ACCOUNTANT'S INDEPENDENCE

Independence rules have been designed to avoid the appearance as well as the reality of impaired independence. Also, the independence rules of the Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB), and the American Institute of Certified Public Accountants (AICPA) Professional Code of Ethics set forth independence rules governing relationships with companies for which CPAs provide attest and certain other services. The range of proscribed relationships covered by those rules is both wide and carefully defined. The rules are quite stringent, and adhering to them has become a matter of course at accounting firms serving companies registered with the SEC.

One of the dominant perceptions driving the enactment of the Sarbanes-Oxley Act was that accountants had, at times, sacrificed auditor *independence* to obtain and maintain lucrative consulting and other business relationships with audit clients. Many lawmakers and their constituents took the view that if auditors are anything less than stringently independent, they will lack *objectivity* in evaluating audit evidence and fall short of the rigorous *professional skepticism* so central to their function as independent examiners of a company's financial statements. When investors and other stakeholders do not believe the auditor to be independent, objective, and skeptical, they may lack confidence in the truthfulness of information disseminated by management. Now, as noted earlier, the financial crisis of 2008 and 2009 has exposed the regulatory naïveté of focusing solely on the auditor in our complex capital markets, and new legislation is again pending in response to perceptions that certain participants, primarily rating agencies, sacrificed independence for market share.

The three linked topics of this chapter are auditor independence, objectivity, and professional skepticism.

SEC FINAL RULES FOR STRENGTHENING AUDITOR INDEPENDENCE

On January 22, 2003, the SEC voted to adopt rules that would fulfill the mandate of Title II of the Act, which called on the SEC to strengthen auditor independence. Section 201(a) of the Sarbanes-Oxley Act, implemented by the SEC under Section 10A(g) of the Securities Exchange Act of 1934, sets out ten nonaudit services that registered public accounting firms are prohibited from providing to issuers for whom they perform financial statement audits:

1. Bookkeeping or other services related to accounting records or financial statements
2. Financial information systems design and implementation
3. Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
4. Actuarial services
5. Internal audit outsourcing services
6. Management functions
7. Human resources services

8. Broker or dealer, investment advisor, or investment banking services
9. Legal services and expert services unrelated to the audit
10. Any other service the PCAOB determines, by regulation, is impermissible[2]

SEC REGULATION OF FORENSIC ACCOUNTING SERVICES

There was much speculation in advance of the final rules published by the SEC about the types of services that would fall under the ninth category: legal services and expert services unrelated to the audit. As the now-published rules read, in an effort to shore up the independence requirement of auditors, Rule 201(c)(4)(x) of Regulation S-X and Exchange Act Rule 10A-2 deem it unlawful for an accountant to provide "expert opinions or other services to an audit client, or a legal representative of an audit client, for the purpose of advocating that audit client's interests in litigation or regulatory, or administrative investigations or proceedings."[3] The rule goes on to explain that this prohibition extends to working behind the scenes to provide assistance and expertise that educate the audit client's legal counsel in connection with a litigation, proceeding, or investigation.[4] Because auditors have legal obligations in their capacity as auditors, this does not, however, preclude the auditing firm from enlisting its own forensic accounting investigators to (1) extend their audit procedures, in essence conducting a separate investigation into the allegations; (2) shadow the audit client's independent legal counsel and retained outside forensic accounting investigators, if engaged; or (3) perform some combination of the two.

Because the SEC recognizes the difference between expert services provided during litigation and forensic accounting investigative procedures performed either at the request of the audit committee (provided litigation or regulatory investigations are not under way) or in support of the audit when suspicions of illegal acts arise, it has permitted certain forensic accounting services under its new rule. In particular, the Commission has provided that auditors can investigate suspected illegal acts at the request of the audit committee in situations *not* involving litigation or regulatory proceedings. If such proceedings begin during the course of the work, auditors may continue the service only if they remain in control of their work. An excerpt from the SEC's ruling in this regard is as follows:

> *We recognize that auditors have obligations under Section 10A of the Exchange Act and GAAS [generally accepted auditing standards] to search for fraud that is material to an issuer's financial statements and to make sure the audit committee and others are informed of their findings. Auditors should conduct these procedures whether they become aware of a potential illegal act as a result of audit, review or attestation procedures they have performed*

---

[2] U.S. Securities and Exchange Commission, "Final Rule: Strengthening the Commission's Requirements Regarding Auditor Independence" (as required by Sarbanes-Oxley Act of 2002 and effective March 31, 2003), 9, www.sec.gov/rules/final/33–8183.htm.
[3] U.S. Securities and Exchange Commission, "Final Rule: Strengthening the Commission's Requirements Regarding Auditor Independence," 19.
[4] Id., 20 and fn. 98.

> *or as a result of the audit committee expressing concerns about a part of the company's operations or compliance with the company's financial reporting system. In these situations, we believe that the auditor may conduct the procedures, with the approval of the audit committee, and provide the reports that the auditor deems appropriate. . . . Should litigation arise or an investigation commence during the time period that the auditors are conducting such procedures, it is permitted for the auditor to complete the procedures underway, so long as the auditor remains in control of his or her work and that work does not become subject to the direction or influence of legal counsel for the issuer. Furthermore, . . . an accountant's independence will not be deemed to be impaired if, in an investigation or proceeding, an accountant provides factual accounts or testimony describing work it performed. Further, an accountant's independence will not be deemed to be impaired if an accountant explains the positions taken or conclusions reached during the performance of any service provided by the accountant for the audit client.*[5]

The passage illustrates that although expert services are deemed to be advocacy in nature and are prohibited under the Act and the rules adopted by the SEC, forensic accounting investigative services performed either in aid of the audit committee's or management's carrying out of its corporate governance responsibilities or in aid of the audit team's satisfying its responsibilities pursuant to GAAS and Section 10A of the Exchange Act (Section 10A) are permissible. Furthermore, the rules do not penalize a proactive management team or board for involving an investigative team. An auditing firm can continue to provide forensic accounting investigative services for an audit client if those services were already under way when a government investigation commenced so long as the auditor controls its work. Also, forensic accounting investigative services related to a violation of internal policy or procedures are appropriate; so, too, is investigation of whistle-blower allegations. Furthermore, the auditors may already be performing investigative procedures if they were the first to detect a suspected fraud and are therefore well placed to conduct forensic accounting investigative work in the event of an investigation, assuming that they use professionals specially trained for such work. The auditing team in place may enable a forensic services team to be deployed more quickly and effectively.

The Commission's rules governing the provision of expert services now prohibit an independent auditor from being engaged to provide forensic accounting services for the audit client's legal representative in connection with the defense of an investigation by the SEC's Division of Enforcement, a litigation proceeding, or other type of government investigation[6] such as investigations conducted by the Department of Justice (DOJ) or the Environmental Protection Agency.[7] This ruling is due to a direct conflict between legal and accounting ethical requirements: Lawyers are required to be advocates for their clients, while accountants performing audit functions are

[5] Id.

[6] For the purposes of its Final Rule, the SEC defines an investigation as "an inquiry by a regulatory body, including by its staff."

[7] U.S. Securities and Exchange Commission, "Final Rule: Strengthening the Commission's Requirements Regarding Auditor Independence," 20.

required to act independently. Were an auditor to be engaged by a lawyer on behalf of an audit client, the auditor[8] would enter into a relationship that is incompatible with the SEC's independence rules. It is not difficult to trigger this prohibition. Once there is an inquiry of a regulatory body, there can be no forensic accounting services provided for the company by the auditor because such services may be perceived to be expert services, unless of course the services commenced before the inquiry occurred.

While the company is busy hiring lawyers and outside forensic accounting investigators to perform an independent investigation and provide for its own defense, the proactive audit firm will not be sitting by, patiently waiting for the findings. The audit engagement partner—working together with a risk management partner, other partners, and the firm's lawyers—is usually planning a strategy for learning the structure and execution of the client's investigation to efficiently and effectively evaluate the ultimate findings of the investigation and the company's remedial action plan as required by Section 10A. As time is typically of the essence because of SEC filing requirements, it usually is best for the audit firm to establish its own plan early in an investigation.

While by no means required to do so, the auditing firm may consider the value of deploying its own forensic accounting investigators. Its forensic accounting investigators would work under the existing audit engagement letter as an extension of the audit scope. The forensic accounting investigators may neither take direction from client's counsel nor aid client's counsel in any manner typical of consultants or expert witnesses working on behalf of the company. Auditors and their forensic accounting investigators are precluded from an advocacy role on behalf of clients—however minimal the role might be. On the other hand, they may share their planned investigative and other audit procedures, as well as their findings, with the client and client's counsel at the direction of the audit committee or special committee charged with overseeing the investigation. Nonetheless, the auditing firm's forensic accounting investigators must be careful not to cross the line between the permitted, expanded audit scope and the prohibited expert services listed earlier.

The introduction of the auditing firm's forensic accountants to the audit when fraud concerns arise may be likened to calling upon tax or pension specialists. The regulations recognize that audit committees, or companies, find it beneficial to engage the auditing firm to perform internal investigations or fact-finding engagements (understood to include forensic accounting investigative work), provided that no expert role in litigation is expected. This is consistent with the overall mission of Sarbanes-Oxley to improve corporate governance. The SEC permits this activity on the part of auditors because it recognizes the positive role that forensic accounting plays in the conduct of a comprehensive audit. It specifically commented that ". . . performing such procedures is consistent with the role of the independent auditor and should improve audit quality."[9] Furthermore, auditors are obligated under Section 10A and under GAAS to assess the risk of fraud that is material to an issuer's

[8] It's important to recognize that "the auditor" is considered to mean the auditing firm and includes all staff working for that firm. Therefore, a forensic accountant of the auditing firm is covered with this prohibition just as the auditor is.

[9] U.S. Securities and Exchange Commission, "Final Rule: Strengthening the Commission's Requirements Regarding Auditor Independence," 20.

EXHIBIT 11.1 Forensic Accounting Services: Prohibited and Allowed

	Services Rendered in Defense of Enforcement Agency Investigation	Services Provided as an Extension of Audit Scope to Assist Current Auditors	Providing Expert or Consulting Services under a Legal Privilege	Assisting Audit Committee with Internal Investigation of Potential Accounting Impropriety[a]
Nonaudit Client	Allowed	Allowed	Allowed	Allowed
Audit Client	Prohibited	Allowed	Prohibited	Allowed

[a]It is not permitted for this assistance to include defending or helping to defend the audit committee, or the company generally, in a shareholder class action or derivative lawsuit, or an investigation commenced by a governmental enforcement agency whether criminal (U.S. Department of Justice) or civil (SEC), unless begun before an enforcement proceeding. Fact witness services are permitted.

financial statements and to plan procedures to address that risk and ensure that the audit committee and others are informed of their findings. Not surprisingly, the audit firm, recognizing the differences between auditors and forensic accounting investigators, may prefer that these extended-scope procedures include the significant involvement of their own forensic accounting investigators, who actually become part of the audit team.

Exhibit 11.1 summarizes which forensic accounting services and fact-finding engagements are prohibited under Sarbanes-Oxley and which are allowed.

CONSULTING VERSUS ATTEST SERVICES

Even before Sarbanes-Oxley was enacted, the accounting profession had clear independence standards in place. Professionals at public accounting firms who provide attest services such as financial statement audits and financial statement reviews [10] as defined in the Statements on Standards for Attestation Engagements[11] are required to be independent of the parties they audit. Auditors were understood to have an obligation to provide unbiased, objective opinions—in view of the fact that their reports are relied upon by third parties, such as the investing public and creditors, who cannot independently verify the results or assess the scope of the auditor's work. Independence in this context is a specifically defined attribute pursuant to AICPA Rule of Professional Ethics 101 (ET Rule 101), which appears in the adjoining box.

[10] In addition to audit and other attestation services, compilations and reviews are considered assurance services and are conducted in accordance, respectively, with GAAS and the AICPA Standards for Compilation and Review Services as adopted by the PCAOB.

[11] For private companies, the Auditing Standards Board (ASB) remains the senior technical committee of the AICPA designated to issue auditing, attestation, and quality control standards and guidance. The ASB develops and issues standards in the form of Statements on Auditing Standards, Statements on Standards for Attestation Engagements, and Statements on Quality Control Standards (together, "ASB Statements").

The categories of direct financial interest covered by ET Rule 101 represent only one element in the relationship between auditors and their clients that raised concerns in the wake of the corporate scandals at Enron and WorldCom.

ET RULE 101

According to ET Rule 101, independence is considered to be impaired during an attestation engagement if:[12]

A. During the period of the professional engagement, a covered member:
1. Had or was committed to acquire any direct or material indirect financial interest in the client
2. Was a trustee of any trust or executor or administrator of any estate if such trust or estate had or was committed to acquire any direct or material indirect financial interest in the client and
   (i) The covered member (individually or with others) had the authority to make investment decisions for the trust or estate, or
   (ii) The trust or estate owned or was committed to acquire more than 10 percent of the client's outstanding equity securities or other ownership interests, or
   (iii) The value of the trust's or estate's holdings in the client exceeded 10 percent of the total assets of the trust or estate
3. Had a joint closely held investment that was material to the covered member
4. Except as specifically permitted in interpretation 101–5,[a] had any loan to or from the client, any officer or director of the client, or any individual owning 10 percent or more of the client's outstanding equity securities or other ownership interests
5. During the period of the professional engagement, a partner or professional employee of the firm, his or her immediate family, or any group of such persons acting together owned more than 5 percent of a client's outstanding equity securities or other ownership interests.

B. During the period covered by the financial statements or during the period of the professional engagement, a firm or a partner or a professional employee of the firm was simultaneously associated with the client as a:

C. Director, officer, or employee or in any capacity equivalent to that of a member of management

D. Promoter, underwriter, or voting trustee

E. Trustee for any pension or profit-sharing trust of the client

[a] Consider also ET Section 101, Rule 101.07.

[12] American Institute of Certified Public Accountants, Code of Professional Conduct, ET Section 101, Independence, Rule 101, www.aicpa.org/about/code/index.html.

INTEGRITY AND OBJECTIVITY

In addition to requirements about independence, ET Section 100 of the AICPA Code of Professional Conduct addresses the issues of integrity and objectivity. ET Rule 102 on integrity and objectivity states, "In the performance of any professional service, a member shall maintain objectivity and integrity, shall be free of conflicts of interest, and shall not knowingly misrepresent facts or subordinate his or her judgment to others."[13] In the eyes of the AICPA and the accounting profession generally, ET Rules 101 and 102 are separate and distinct from one another. Independence is defined narrowly and codified by ET Rule 101. Integrity and objectivity are also specifically defined and codified by a separate list of rules (ET Rule 102). The wave of corporate scandals demonstrated the critical importance of all three concepts: independence, integrity, and objectivity.

Independence Standards for Nonattest Services

Rule 101 recognizes that the independence of auditors engaged in attestation services is impaired if they do not meet the requirements noted in the aforementioned sidebar. In contrast, accountants at public accounting firms who provide nonaudit services (practitioners), such as litigation or forensic accounting services, remain independent pursuant to ET Rule 101—and in particular pursuant to Rule 101–3—without considering the requirements in the sidebar. The role of the practitioner who delivers attest services is quite different from the role of the practitioner who provides litigation and forensic accounting services. In attest services, the auditor assesses the fairness of the assertions of others—such as in financial statements—whereas in litigation engagements, the practitioner renders an expert opinion or provides other consulting services based on expert analysis, judgment, experience, education, and so on. Moreover, the results of attestation engagements are relied upon by third parties who cannot investigate the validity of the opinion expressed, while in litigation engagements, the opposing party has the opportunity to closely question the expert's findings, methods and procedures, education, and experience.

As stated in ET Rule 101: "Investigative services include all forensic services not involving actual or threatened litigation such as performing analyses or investigations that may require the same skills as used in litigation services. Such services would not impair independence provided the member complies with the general requirements set forth under this interpretation. Expert witness services create the appearance that a member is advocating or promoting a client's position. Accordingly, if a member conditionally or unconditionally agrees to provide expert witness testimony for a client, independence would be considered to be impaired. However, independence would not be considered impaired if a member provides expert witness services for a large group of plaintiffs or defendants that includes one or more attest clients of the firm provided that at the outset of the engagement: (1) the member's attest clients constitute less than 20 percent of (i) the members of the group, (ii) the voting interests of the group, and (iii) the claim; (2) no attest client within the group is

[13] American Institute of Certified Public Accountants, Code of Professional Conduct, ET Section 102, Integrity and Objectivity, Rule 102, www.aicpa.org/about/code/index.html.

designated as the "lead" plaintiff or defendant of the group; and (3) no attest client has the sole decision-making power to select or approve the expert witness. As such, a practitioner performing investigative services will have certain independence considerations. Specifically, the practitioner should be aware that in some instances, if the practitioner provides audit services, they may be precluded from providing litigation services."[14]

PROFESSIONAL SKEPTICISM

The AICPA Code of Professional Ethics requires member auditors to address professional skepticism as follows:

> *Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. The auditor should conduct the engagement with a mindset that recognizes the possibility that a material misstatement due to fraud could be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity.*[15]

Throughout this book are examples where the appropriate level of professional skepticism was absent from the minds of the auditors. Imagine how certain corporate scandals might have been different had the auditors brought a greater degree of objectivity and professional skepticism to bear on gathering and evaluating sufficient competent audit evidence to ensure that the accounts were stated fairly and in accordance with the professional standards applicable at the time (both the AICPA and the Institute of Internal Auditors) governing reasonable assurance.

Being hit by fraud is much like being hit by lightning. While we all know that people get hit by lightning, it is an unlikely event for any particular person. Most of us take precautions—but in reality, we do not dwell on the possibility that we may get hit by a lightning bolt. However, those who have been struck by lightning and survive are certain in the future to take every reasonable precaution. So it is with victims of fraud. An auditor and the auditor's client are likely never to have been defrauded at all or to a significant extent. They take standard precautions against fraud because they know that fraud can occur; they follow the relevant professional standards. Even though the rate of incidence of material financial statement fraud is only 2 percent, auditors' professional standards require auditors to practice professional skepticism at all times.

---

[14] American Institute of Certified Public Accountants Professional Standards Code of Professional Conduct, ET Section 100—Independence, Integrity, and Objectivity, ET Section 101 Independence, May 12, 2005, with footnotes added, effective February 28, 2007, by the Professional Ethics Executive Committee.

[15] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, "Consideration of Fraud in a Financial Statement Audit" (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par. 13.

In organizational life, few things are more distressing than witnessing the painful aftermath when a trusted employee is shown to have perpetrated a fraud. For example, a not-for-profit organization recently learned that one of its trusted employees, who had joined the organization immediately after high school and stayed for 30 years, was responsible for a whole series of scams to defraud the organization. The investigation identified three distinct scams totaling $1.4 million. (See Chapters 22 and 23 on fraudulent schemes.) Unfortunately, the employee fled the area, and the organization is unlikely to make any recovery.

Understandably, the organization's executive director was beside himself with anger and filled with a sense of betrayal. When forensic accounting investigators first met with him, they could see that his attitude was undergoing radical change as he attempted to come to grips with this violation of trust. Lightning will not strike him twice. He is a changed man. He will trust—but he will verify for the rest of his days.

TRUST BUT VERIFY: A CASE STUDY

Many forensic accounting investigators have had an episode in their careers that changed forever their perspective on trust. The following narrative recalls that moment of truth for a young auditor confronted for the first time with material fraud.

In the early years of his career as an auditor, before becoming a forensic accounting investigator, he liked to say that he followed his mother's advice to trust others unless there was good reason to mistrust. He had no notion that a criminal would ever cross his path or do serious financial harm to a company he was auditing. He was naive: One of his audit clients was destroyed by fraud, and the overall experience converted a competent young auditor into the founder of a specialized forensic accounting investigations practice.

In the mid-1980s, he was assigned to participate in the audit of a public company in the high-tech industry, which had gone public two years earlier. This particular year was the third audit cycle. As he went about his work, the young auditor encountered an anomaly in the lease-contracts receivable[16] (LCR) accounts he was examining. While wrapping up his audit procedures in the LCR area, he was having a conversation with an accounts receivable clerk in the office—and happened to notice on that individual's desk a fairly thick file labeled *Complaints*. Walking back to his desk, he found himself thinking about that file. Why, he asked himself, would there be a file like that in a company that is growing at an industry-leading rate and highly regarded by the capital markets and the financial press?

That evening, he took a closer look at that file.[17] What he found was shocking. The file was filled with what amounted to hate letters—at least a hundred letters from

[16] Lease contracts receivable is the asset created when a lease is capitalized as required by ASC 840–10–45–2,3 "Broad Transactions, Leases, Overall, Current Value Financial Statements." Similar to an accounts receivable, the asset is decreased by monthly lease payments.

[17] The company had previously given the auditors access to such files in recognition of the fact that the auditors worked late and, in the interest of efficiency, did not wish to require them to wait until company staff returned the following day. Hence, the company staff was requested by the company to make accessible to the auditors all files pertaining to the accounts.

angry customers stating that the company's products were inferior and demanding that the company's alarm system product be pulled and their contracts canceled. Recovering his mental poise, the young auditor began asking himself how it could be that when he had recently circularized a population of 15,000 leases and selected several hundred of them for positive confirmation, he had not randomly selected even one of these unhappy customers. The odds seemed reasonable that he would have selected at least one irate customer. Even if the odds were not all that good, there was something here worth looking into.

The following day, he took it upon himself to extend his audit procedures to determine whether there were other customers upset with the company.[18] Besides the newly discovered Complaints file, there was nothing in the testing results that warranted such an audit step—except his intuition. He went forward with the additional testing. From the Complaints file, he randomly selected five letters demanding that the company's equipment system be pulled and the contract canceled. All were dated prior to year-end. Giving the list of five names and addresses to an LCR clerk, he asked the clerk to furnish a phone number for each customer, because he wanted to speak directly with these customers to confirm their issues with the company. He did this without explanation as to why the audit scope had just been expanded.

He had, in the normal course, already sent out several hundred confirmations to customers but had not received back any exceptions. This, too, seemed odd, particularly because this newly minted public company was growing rapidly and systems and controls were straining to keep up with the pace of growth. The company appeared to be managing well enough, but it still seemed strange that not one customer took exception to any contract information or complained in any way during the standard confirmation procedure. Until seeing the Complaints file, he had not given this situation a second thought.

Within an hour, the young auditor received copies of the customer names and telephone numbers, as he had requested. Oddly, the information had been photocopied from the precise pages in the LCR subsidiary ledger that had been his control copy supporting the asset balance for LCR accounts as of the audit date. He reread all of the information about the assets and unearned balances relative to each lease—and abruptly realized that if the customer's letter requested cancellation of the contract and removal of the system *before year-end,* then the proper accounting procedure would have been to remove the asset from the balance sheet and write off the remaining balances. There was no evidence this had been done for the five customers picked at random from the Complaints file, nor did there appear to be any reserve account serving the same purpose. The LCR subsidiary ledger was reconciled to the general ledger—proving to him that the net asset balances for those five customers were recorded in the financial statements. This was wrong. They should have been written off.

Now the young auditor became anxious. Not wanting to leave until he had resolved the situation, he continued his examination. Adding to his concern, none

[18] This matter predated both SAS 82 and SAS 99 and, of course, enactment of the Sarbanes-Oxley Act. The auditor's actions today would be different, given the new standards and regulations as well as subsequently improved training on specific protocols to follow when fraud is suspected.

of the five customers had been selected for positive confirmation. Because they were part of a population of about 15,000 leases, this was not too worrisome; nonetheless, it was a fact. The thing to do next was to call these former customers and verbally confirm the details in their letters.

What better time to do this than that very evening? The company was planning to release earnings in three days, and the audit process was all but complete. A voice inside the young auditor insisted, "There is a reasonable explanation for all this. You are missing something and wasting time." In spite of that internal message, he continued investigating.

One by one, each of the five customers confirmed the details in their letters. Each had had the company's equipment system pulled and the contract canceled before year-end. Then why, the auditor asked himself, was the asset still listed at year-end? There was no write-off, no reserve, no reconciling item between the general ledger and the financial statements. His attention was drawn back to his circularization procedures, and he decided to reperform the selection process manually. An audit intern had looked after these procedures in the first round, but now the auditor had to see for himself. Knowing the random start and the interval used for the positive confirmation selection process, he began counting manually. He began counting his way through the subsidiary listing of 15,000 customers. Hours passed. He continued manually counting the interval of every fiftieth customer. Then, at about 3 A.M., he hit the fiftieth count on one particular customer and noted that it was not selected for confirmation. The selection process was computer automated. Computers do not make these kinds of mistakes.

Feeling that fatigue was causing him to make mistakes, he recounted and got the same result. He copied the name and other relevant balance information on this fiftieth customer who was mysteriously not selected for positive confirmation and proceeded to leaf through the Complaints file in search of the name. The letters in the file were in no particular order. It took awhile to find the name, but find it he did: a letter dated in August from a lease customer requesting that the equipment system be pulled and the lease contract canceled. As of December 31, the asset representing this customer and lease was still included on the LCR listing and, accordingly, included in the company's financial statements.

He had found just this one. From the perspective of materiality, it was valued at only about $3,500 net of the unearned revenue portion and deferred monitoring costs. On a balance sheet of about $50 million, this was certainly no showstopper—but then, he was just getting started.

He continued his count and soon found others with the same characteristics. By 8:30 A.M., when the company's staff began arriving for their day's work, he had found a total of seven for which there was a complaint letter demanding that the company remove their equipment system and cancel the contract, yet the asset was still listed in the year-end LCR asset listing. This manual review had covered less than 10 percent of 15,000 leases, but the auditor had learned enough to go on to the next step. He asked one of the company's information technology (IT) staff members to print out every column in the electronic file for each of these seven customers. Examining that printout, he noticed there were some 15 fields detailing customer information such as customer number, name, phone number, and asset and liability balances. This was the same information listed in the LCR subsidiary ledger. However, on this new listing, in the far right column, there was a *Z* for each

of the seven.[19] No caption at the head of the column made clear what *Z* signified. It was the only common characteristic among the seven. The auditor asked the IT staffer to perform a query on the entire LCR master file: He wanted all customers listed out who had that *Z* in their customer file history at December 31.

Hours passed. Once the staffer had brought the report, it seemed clear to the auditor that the staffer must have misinterpreted the request, because the report was very long. Upon closer examination, it became evident that the query, correctly conducted, had captured nearly 4,000 customers with an aggregate net LCR balance of just under $11 million. For a company with $7 million in pretax net income, the $11 million was obviously material to the financial statements and promised to be a highly significant discovery.

The auditor still refused to believe the result of his examination. He went home, rested, and mentally reviewed every step of the procedures performed in the past few days. He could not find a procedural flaw, and he could not argue away the ominous implication of the findings. He got in touch with his engagement partner and reported the findings. After several internal conversations and review, the partner relayed the findings to senior company executives and the board of directors. This set in motion a seven-week investigation, led by the young auditor, to determine the extent of the fraud he had single-handedly uncovered. Who was involved? How large in dollar terms was the accounting fraud? What years were affected? How did it escape detection? What effects would these discoveries have on the company and on the auditing firm?

After completing this thorough investigation, the audit firm withdrew its prior-year opinions. Not surprisingly, the SEC Division of Enforcement took notice and rapidly issued subpoenas directed at both documents and persons, including the young auditor. As the consequences of the fraud played out, the company stock was delisted and the company eventually filed for bankruptcy.

The young auditor had experienced his moment of truth and learned the meaning of professional skepticism. However, the moral of the story is not to withhold trust. It is to trust—but verify.

Trust but Verify: Exploring Further

We owe the expression *trust but verify* to President Ronald Reagan, who used it during the Cold War to define the U.S. position on missile systems inspection. *Trust but verify* should be the credo of all auditors as they perform their duty of ensuring that the information disseminated by management properly depicts the financial condition of the company being audited. We all know what *trust* means, but the word *verify* may need clarification.

We can start with its definition. Merriam-Webster defines *verify* as a verb that means *to confirm or substantiate; to establish the truth, accuracy, or reality of*. Defined in this way, the word is not a specific term of art in the world of auditing.

[19] Later, it was determined that someone at the company had changed the program of the tape used to select customers for confirmation. Essentially, when the fiftieth item selected had a Z in the record, the program change permitted that customer to be skipped over, selecting instead the fifty-first customer for confirmation.

Instead, we refer to the process of verification in terms of ascertaining the completeness, accuracy, and validity of a transaction, of groups of transactions, or of balances.

- *Completeness*. Whether all transactions and other events and circumstances that occurred in a specific period and should have been recognized in that period have in fact been recorded.[20]
- *Accuracy*. The correctness and appropriateness of a statement, account, set of accounts, or document—such as a voucher—in portraying facts or opinions whose degree of accuracy is measured by the relative correspondence of a statement, account, or document to the facts. Accuracy is a close cousin to *validation*.[21]
- *Validity*. Involves the actual occurrence and approval of transactions, as well as relevancy, truth, correctness, and enforceability. *Validation* is the determination of whether a test yields desired results with the necessary elements of accuracy, precision, reliability, and relevance.[22]

Verification is the means by which an auditor gathers sufficient auditor evidence. Yet auditors cannot in all reasonableness mistrust their clients. If clients were not trusted, they would not be clients for very long. However, the auditor's trust should be supported by whatever processes of verification are appropriate under given circumstances. An auditor who adheres to the practice of trusting but verifying should not rely on the presumed character of any individual who creates a transaction or has responsibility for an important control function without ascertaining, on an independent and objective basis, the accuracy, validity, and completeness of the matter under review. Paragraph 13 of Statement on Auditing Standards (SAS) No. 99 addresses the issue of trust and honesty:

> *Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. The auditor should conduct the engagement with a mindset that recognizes the possibility that a material misstatement due to fraud could be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity. Furthermore, professional skepticism requires an ongoing questioning of whether the information and evidence obtained suggests that a material misstatement due to fraud has occurred. In exercising professional skepticism in gathering and evaluating evidence, the auditor should not be satisfied with less-than-persuasive evidence because of a belief that management is honest.*

The basis for trust must be verification of the underlying financial data and not any prior experience with management. Even seemingly honest people can defraud,

[20] Robert Hiester Montgomery, *Montgomery's Auditing,* 12th ed. (New York: John Wiley & Sons, 1998), 6–1.
[21] Eric Louis Kohler, *Kohler's Dictionary for Accountants,* 6th ed. (Englewood Cliffs, N.J.: Prentice-Hall, 1983), 18.
[22] Id., 528.

depending on current-year incentives, opportunities, and the ability to rationalize one's actions.

Paragraph 15 of SAS 99 indicates that any prior impressions of management's integrity should have no bearing on the current-year audit. In a parallel to the concept of zero-based budgeting, the auditor must reassess the environment for fraud each year:

> *The discussion among the audit team members about the susceptibility of the entity's financial statements to material misstatement due to fraud should include a consideration of the known external and internal factors affecting the entity that might (a) create incentives/pressures for management and others to commit fraud, (b) provide the opportunity for fraud to be perpetrated, and (c) indicate a culture or environment that enables management to rationalize committing fraud. The discussion should occur with an attitude that includes a questioning mind as described in paragraph 16 and, for this purpose,* setting aside any prior beliefs the audit team members may have that management is honest and has integrity. *In this regard, the discussion should include a consideration of the risk of management override of controls. [*emphasis added*]*

While determination of the appropriate audit procedures is usually a facts-and-circumstances undertaking, the following examples of the practice of trust but verify can shed useful light on making that determination.

Example 1

Auditor Observation Several significant accounts receivable have been re-aged, there is no valid documentation supporting such a practice, and the practice of re-aging is not permitted by company policy. The auditor presents the issue to the client for explanation.

Client Response We noticed this problem several weeks ago in preparing for the audit, and we are in the process of correcting it. The amounts are not material. During a system implementation, there were some glitches in the accounts receivable program, but they are now fixed.

Potential Auditor Responses The auditor who trusts but verifies may consider performing the following steps:

- Interview the employee who first noted the problem.
- Interview the IT technician who worked on the fix, and confirm the company's message about the nature of the problem.
- Extend testing in the aging of accounts receivable to verify that the matter is (1) immaterial as indicated and (2) corrected, with all appropriate adjustments made.
- Reevaluate bad debt reserve, which may have been understated due to re-aging of the invoices.

Example 2

Auditor Observation While performing sales cutoff testing procedures during year-end audit procedures, the auditor discovers a large number of invoices marked *Bill, but do not ship. See George.*

Client Response These invoices belong to our largest client in Germany. Given that storing costs are astronomical in Germany and that the client is able to obtain inventory from our independent warehouse facility within one day, we believe that the arrangement and recognition of these sales are appropriate.

Potential Auditor Responses Upon receiving this verbal response, the auditor may consider requesting supporting documentation, such as purchase orders, sales agreements, and bills of lading. The auditor keeps in mind that a sale should be recognized only once the risk and rewards of the transaction have been transferred, the amount of the sale is determinable, and the collectibility of such sale is not in doubt. In addition to items that may not be mentioned further on, the auditor may consider performing all or a portion of:[23]

- Make inquiries of management and employees who are approving and generating these transactions.
- Select a sample of recorded sales, review their terms to assess reasonableness, and confirm such with your customers.
- Examine and assess for validity the existence and appropriateness of supporting documentation for each selection.
- Select a sample of shipping documents, and trace back to the open-accounts-receivable report.
- Review prior- and current-year January journal entries, specifically for sales reversals related to bill-and-hold invoices.
- Make inquiries of management regarding the agreement between management and the warehouse facility.
- Independently confirm your understanding of the client's arrangement with the warehouse facility by specifically asking the following of the warehouse manager:
  - Who is in control of the inventory while staged at the warehouse facility?

[23] Please note that this roster of audit steps is not exhaustive; other steps might also be needed in an actual situation. The applicable SEC guidance is Staff Accounting Bulletin 101, also referred to as Topic 13-A, which addresses revenue recognition under the following criteria, cited verbatim: The staff believes that revenue generally is realized or realizable and earned when all of the following criteria are met:

Persuasive evidence of an arrangement exists;

Delivery has occurred or services have been rendered;

The seller's price to the buyer is fixed or determinable; and

Collectibility is reasonably assured.

- Does your customer (the audit client) ever inform you that the buyer has canceled the order and request that you refrain from shipping?
- How often is inventory returned?

If everything checks out, you would normally move on in your audit program. If there are discrepancies to the extent that you question the truthfulness of the client representative who initially explained the problem and its solution, it is often wise to consult with a forensic accounting investigator before confronting that representative: It is usually a tactical error to confront client personnel with suspicions before consulting with an expert on fraud and deceit. (See Chapter 12 on common missteps.) All too often, a fraudster may play the auditor by simply calling the matter a misunderstanding or brushing it off with: "I'm sorry. I must have misspoken."

LOOSE-THREAD THEORY OF AUDITING

The loose-thread theory postulates that in most frauds there are indications of the defalcation that could reveal the *nature* of the offense, although not its *total impact*. If such indications—or, in the technical language of the field, *indicia*—are recognized on a timely basis and investigated in an appropriate manner, they may identify an even larger fraud, perhaps material to the financial statements taken as a whole. By definition, loose threads are usually small and easily overlooked. As discussed in Chapter 13, on warning signs, they are ignored at grave peril.

An illustrative example will be helpful. An audit firm was completing a rotational audit of a small division of a large apparel manufacturer. With $28 million in total assets and $23 million in annual sales, the division was one of 60 such divisions around the world. The most recent external audit procedures had been performed at this division four years earlier. The parent company was a long-term client of the audit firm and had never been found to have noteworthy problems in its financial statements. The division CEO paid close attention to his unit's operations, scrutinized all financial reports, and tracked both revenue and expenses to budget on a monthly basis. In all of these respects, the division was much like thousands of other divisions of global companies.

On a consolidated basis, the parent company had $750 million in total assets, with annual sales stabilizing at $300 million after a nearly five-year slide from $650 million. The company had taken some huge expense charges in the previous two years to downsize operations and improve the bottom line. In the current year, consolidated pretax net income was $21 million after a loss of $44 million the previous year. All things considered, it looked like a reasonably good year for the company, and management was ready to take its bows at the upcoming shareholders' meeting.

The audit team at that modest division came across a customer confirmation that took exception to its accounts receivable balance as reflected in the accounts receivable subledger at December 31. This subsidiary ledger was the source used for selecting customers for confirmation of amounts owed to the company. In the confirmation, the customer disputed an invoice for $22,000, claiming it had been paid several months earlier. The staff auditor called the customer and received

confirmation that the invoice had been paid; a faxed copy of the canceled check dispelled any remaining doubt. The auditor suspected that a small oversight had obviously occurred, but there was no reason for concern. He would simply mention it to Fran, the controller and top financial person at the division. It was just a loose thread.

Fran had been at the division for 26 years. Fran was well liked, trusted, and married to the division's IT manager. They had two children. The family lived in the home she had been raised in, the couple was happily married, and the two of them obviously enjoyed and valued their jobs at the company. The auditor was confident that Fran could set things right in short order.

This was the staff auditor's second year on the audit. The audit manager communicated to the staff auditor that he had worked with Fran four years ago and found her to be competent, helpful, and pleasant. When the staff auditor approached Fran with the confirmation exception and asked her to resolve it, she said she would get right on it. The next day, she met with the staff auditor and explained that the discrepancy had occurred in April, a month during which the system had crashed and several resulting problems later came to light. She said she would scrub the entire accounts receivable subledger to ensure that there were no other problems and would report back in a day or two. That timing put resolution of the matter on the last day of fieldwork, but the staff auditor was confident that Fran would follow through because, according to the audit manager, she had always done so in the past.

True to her word, Fran returned to the staff auditor on the last day of fieldwork with four similar discrepancies totaling $53,000 in customer payments that should have been credited off but had not been. The original credits actually went to the cost-of-goods-sold account. Fran reported with a surprised smile, "I have no idea how that happened." She assured the staff auditor that the credits would be reclassified as of December 31 and apologized for the oversight. The total income statement effect was immaterial on both division and consolidated bases. Reviewing the additional payment misclassifications, the staff auditor noted that none of them was selected for confirmation. He discussed the matter with the engagement manager, who in turn consulted with the engagement partner. All agreed that the matter was immaterial, but they had less comfort than before and decided that additional work would need to be performed before they could sign off on the accounts.

While all this was occurring, the audit manager was also winding up her work at the division by completing a review of accounts payable and accrued liabilities—and she noted some concerns. Although the accrued expense balances appeared to be in line with prior periods and other measurements, there were a few unfamiliar accounts designated as "retailer allowances." The audit manager questioned Fran directly about these entries, and Fran both minimized the issue and complained that she was short-staffed and already working on resolving the accounts receivable issue brought to her attention a few days earlier. She said she would get to the accrued-expenses questions—but probably not until next week. However, "next week" was close to the audit committee meeting and the parent's intended earnings release date. The manager was uncomfortable with that plan and said as much to the company's regional controller. He agreed that speed was of the essence and sent his assistant at once to help Fran resolve this and any other problems that required attention before the auditors could leave.

Fran's accounts were receiving a lot of attention. This did not make her happy, and she was not shy about expressing her displeasure. The Fran whom the auditors had known for years had become a very different person. She wanted the auditors out. But the closer the auditors looked, the more issues and questions surfaced. The audit engagement partner, becoming suspicious, got in touch with a forensic accounting investigator, who sent two forensic accounting investigators to the division on the following day. Examining four electronic files—payments, employee master, vendor master file, and journal entries—with the use of forensic software applications, they identified many questionable transactions.

The audit engagement partner had seen enough. He recommended to the parent company's chief financial officer (CFO) that he should strongly consider postponing the company's earnings release. Not surprisingly, this was the last thing the CFO wanted to hear. Only a day or two earlier, he had been told everything appeared to be fine for the planned earnings release date.

What transpired from that point was an avalanche of discoveries and events. Two additional auditors and two additional forensic accounting investigators arrived on the scene. Management's jubilation over its comeback year was quickly dissipating, as the income statement impact of this relatively small division began to become apparent. At the end of that first week of forensic investigation, the total hit to income amounted to $6 million pretax. At the end of the investigation two weeks later, the final tally was $11 million—just over half of the company's consolidated pretax net income. This was material by any measure.

Although the numbers were now sound, the auditors had not yet completed their work. The forensic accounting investigator had informed the audit team that Fran was a fraudster, and the task at hand was to look at everything within her reach and formal span of responsibility. Were there additional schemes extending beyond the books and records—for example, bribery or kickback schemes? The fact that Fran's husband was the IT manager also made his activities fall under additional scrutiny. The last thing the parent's CFO wanted was to extend the investigation, but he realized he had no choice in the matter if he wanted the auditors to sign off. In due course, the forensic team conducted an admission-seeking interview with Fran and determined that she had not engaged in any additional schemes, but it became clear to them that she was withholding information likely to incriminate the division CEO. He in turn became a suspect, and the same process was repeated: examination of everything he touched followed by an admission-seeking interview.

It was critically important to follow up on leads and identify every culpable employee. If this fraud could be isolated to the division, then the team had completed its work, but if, for example, investigation of the division CEO revealed that he had conspired with someone at corporate headquarters, then the investigation would have to continue until all culpable parties were identified and the fraud contained and quantified.

The auditors completed their procedures, including an assessment of previously performed procedures at corporate and other divisions. Once the company had assessed that it had identified the total extent of the fraud, corporate management issued a press release. Its share price dropped 20 percent on the news, and SEC Enforcement immediately began an informal inquiry. As of the time this chapter was written, the stock had not yet recovered. The two miscreants were terminated and the government's investigation is proceeding.

Recognition of a loose thread had led to discovery of a high-impact, multimillion-dollar fraud. Who was defrauded? Many individuals along the line were fooled by the numbers, but ultimately, it was the investors from whom accurate information about the company's revenues had been concealed.

FURTHER THOUGHTS ON THE LOOSE-THREAD THEORY

The preceding case study demonstrates—as would many, many others—that a small anomaly may be a sign of fraud. The *loose-thread theory* could not be more appropriately named. Fraud is usually hidden, and the discovery of fraud usually is unlikely, at least at the beginning, to involve a huge revelation.

Financial fraud occurs in manipulated accounts, but it has some points in common with a crime scene. You suspect a crime has been committed, and there is a room you believe the crime occurred in. Picture yourself walking into it. You slowly pan the room for clues. You would certainly not expect to see someone sitting in a chair in a corner of the room holding a sign saying: "I stole $2 million. Just ask me, and I'll tell you how I did it." Ultimately, that admission is your objective, but there is much work to do before scheduling an admission-seeking interview (see Chapter 16). Like loose threads on clothing, the clues you need are easily overlooked.

An audit does not presume that those you interview and the documents you examine have something sinister about them. The overwhelming majority of audits are conducted in companies in which material fraud does not exist. However, the auditor is always aware that material fraud could be present. In some respects, steady maintenance of professional skepticism is a more difficult challenge than responding to a crime you know has occurred. Imagine walking down a dark alley into which you know a suspect has entered just before you. You do not know where the suspect is, but as you walk down that alley, you are acutely aware of and attuned to your surroundings. Your senses are at their highest level. You know beyond the shadow of a doubt that danger lurks nearby.

Audits are not like that. Audits are more like walking through a busy mall and watching normal people go about their daily activities. In the back of your mind, you know that among all the shoppers are a few—a very few—shoplifters. They look just like everyone else. You know they are there because statistical studies and past experience have shown they are there, but you do not know exactly where or who they are or when you will encounter them, if at all. If you were engaged to find them, you would have to design procedures to increase the likelihood of discovery without annoying the great majority of honest shoppers. So it is with an audit. If an audit firm *knew* that management was engaged in fraud, it would not accept the audit engagement in the first place or would withdraw while complying with all applicable standards of performance and regulations. Professional skepticism is a key practice in a context in which the auditor has reason to trust—but also reason to verify.

As noted earlier, many perpetrators of fraud have no desire to harm others. When apprehended, most white-collar criminals are typically—and sincerely—regretful that the frauds they've perpetrated cause others to lose security, careers, investments, or savings. That most financial fraudsters execute their devious strategies without intent to harm actually complicates the task of the auditor in discerning

the validity, completeness, and accuracy of the information provided to them in the normal course of an audit. The auditor's guard must always be up. If there is a hidden fraud operating in a company, the path to its discovery will often be littered with tiny loose threads rather than large neon signs. Professional skepticism is the attitude most likely to detect those loose threads, understand their meaning, and, when appropriate, set in motion a forensic investigation performed by competent forensic accounting investigators.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 12

Potential Missteps: Considerations When Fraud Is Suspected

Thomas W. Golden and Kevin D. Kreb

This chapter explores some of the unintended consequences that may arise when well-intentioned, competent auditors and company executives detect the possibility of fraud and understandably want to reach an immediate resolution. A good knowledge of the more significant potential missteps should help both auditors and their clients in the proper conduct of an investigation. As discussed in earlier chapters, when there is a suspicion of fraud, the surest path is to employ appropriate experts and to do so early. Most of the missteps put the natural desire to shed immediate light on the problem ahead of the painstaking professional approach that is far more likely to uncover the truth, expose the issues to the fullest possible extent, obtain desired legal outcomes, improve control remediation efforts, and increase recoveries.

CONFRONTING SUSPECTS

One step commonly taken by executives or auditors untrained in fraud investigation is to confront a suspect with certain facts immediately after discovery. Such executives or auditors are understandably eager to resolve the apparent discrepancy and take what they believe to be the quickest path to resolution, but they may unknowingly complicate future investigation and actually increase the cost of resolving the allegations. By way of illustration, consider the following. A corporate controller is reviewing quarter-end journal entries and notices several large entries that do not make sense. He retrieves the supporting documents and notices not only that his signature has been forged but also that the documents bear no relation to the entry. He believes the assistant controller made the entries to cover up a defalcation. The controller is naturally upset. He discusses the matter with the chief financial officer, a human resources representative, and an attorney from the general counsel's office. All agree the entries look bad, and the decision is made to confront the assistant controller with the facts to "get to the bottom of this matter." Consulting with a forensic accounting investigator does not occur to them.

The controller summons his assistant to his office and confronts him with the facts and evidence. The assistant controller is by and large silent, taking it all in and periodically asking questions to clarify details. In fact, while the assistant controller

remains calm, his superior is visibly upset. The controller continues laying out the facts for about ten minutes while the assistant controller quietly follows along. Finally, the controller reaches the end of his recitation of facts and suspicions and asks: "What's going on here? What's being hidden?"

The assistant controller has at least two choices: first, he can say to his boss: "I'm really sorry about this confusion. I understand why you're upset. Let me take this back to my desk. I'll figure it out and get right back to you. It will be my top priority today." The assistant controller exits with an armful of the "evidence" that his boss has laboriously assembled and will soon be doing who knows what with it. The controller meanwhile is relieved; he feels he has handled the situation like a good manager. He returns to his work and awaits a response. Later confrontations yield little more—until a week later, when the assistant controller resigns through an e-mail.

Under the second scenario, the assistant controller says nothing. Thinking this strange, the boss prompts him for a response, receiving a mumbled, "I'm not feeling well." The assistant controller tells his boss he is going home sick and will address the issue in the morning. The controller is very unhappy with this response, berates his subordinate for creating the situation, and demands that he make some statement about it then and there. The assistant simply reiterates that he is not feeling well and walks out. The next morning, the controller listens to a voice mail from his assistant saying he is still under the weather, is taking a sick day, and has a doctor's appointment later. On the following day, no assistant controller, no voice mail, and the formerly trustworthy assistant is not even answering his home telephone.

By directly confronting the miscreant, the controller believed he was doing the right thing. However, never having confronted someone skilled at deceit and cover, as the assistant controller apparently was, the controller was soon out of his depth. In such a situation, he may have been better off to have consulted with a forensic accounting investigator. Unknowingly, the controller had conducted an admission-seeking interview (see Chapter 16). A trained forensic accounting investigator knows that this type of interview is often most effective *after* a thorough investigation has been performed, when the interview or series of interviews can be carefully scripted and always conducted with a prover[1] in attendance. Without intending to do so, the controller alerted the miscreant to the fact that he would be exposed, thus making further investigation both difficult and costly. Also, the assistant controller's unresponsiveness on the day after the interview signaled that he had probably fled. That in itself significantly reduced the likelihood of recovery.

The moral of the story, as in any situation in which evidence is found indicating a suspicion of fraud, is to consider consulting with a forensic accounting investigator early on. Suspicion is sufficient reason to do so. We all are naturally curious, and managers often are proud and intelligent individuals, unlikely to feel that a situation cannot be directly addressed and resolved. But reliance on forensic expertise may be critical in achieving the desired result: identification of all of the perpetrators, determination of the extent of fraud, analysis of the pattern of fraud and the faulty controls that permitted it, and recommendations for deterring such fraud in the future.

[1] As explained more fully in Chapter 16, it is best to include a colleague in the interviews who can vouch for what was said, by whom, and when. Without this prover, the suspect can later recant an admission, and then it is the interviewer's word against the suspect's.

Here is another case that illustrates the inadvisability of immediate confrontation. A forensic accounting team recently completed an investigation in the Middle East. The company, a U.S. multinational manufacturer of heavy equipment, had received an anonymous letter alleging that certain employees in the purchasing department—two in particular—were soliciting bribes and accepting kickbacks from vendors. This practice was alleged to have been occurring for a number of years. The forensic accounting investigators were asked to uncover the truth.

Kickbacks are often the most difficult of allegations to prove. The most compelling proof is an admission by the recipient or the vendor. However, both parties are profiting from the corrupt action and have no incentive to tell the truth. Furthermore, kickbacks are not usually paid in front of witnesses; there is little, if any, documentation to establish that they have occurred; and they're usually paid in cash. For these reasons, they're difficult to trace. Kickbacks may greatly increase costs over a period of time, and those costs are often not at all obvious in the records.

In this particular investigation, a confession was not forthcoming. However, after conducting a number of interviews and performing procedures focused on detail, including document examination, the forensic accounting team did identify suspicious e-mails, purchase order violations, and evident lies. They also received two additional anonymous allegations by e-mail. Essentially, they had smoke but no smoking gun—at least none they would describe as solid proof of a kickback. Nevertheless, they had learned enough to believe that most of the allegations in the anonymous letter were true. They just could not prove it yet.

Everyone with whom the forensic accounting investigators talked believed that the two targets were accepting kickbacks, but the targets did a good job of hiding the trail. In the end, the forensic accounting investigators identified several key witnesses who provided enough facts and documents for the team to confront one of the suspects. He in turn incriminated the purchasing supervisor. In an admission-seeking interview, the purchasing supervisor confessed. He lost his job and identified all of the vendors paying bribes. The company has pursued recovery from those vendors.

The investigation took seven weeks to complete and cost the client about $250,000 in fees and expenses. Senior management recognized the value of using forensic accounting investigators. However, the division manager of procurement in the Middle East disagreed with the forensic accounting team's approach and spoke with the members after they had been onsite for about two weeks. He suggested that if he were conducting the investigation, he would simply have confronted the targets with the anonymous letter on the first day of investigation to see whether they would admit to the allegations and thus save the time and money allocated to the investigation. He also floated the idea that the forensic accounting investigators could have confronted the alleged wrongdoers by telephone—in this way saving the money that had been spent on travel to the Middle East. Were they to have made no admission, he argued, the team should then have conducted an investigation onsite.

The forensic accounting investigators agreed with him that investigations should be conducted in the least time-consuming and most inexpensive manner, provided that the desired result was consistent with the methodology used. Here, senior management had explicitly asked for all reasonable efforts to produce the clearest possible outcome—a positive and knowledgeable disposition of the allegations—and any ambiguity in resolving the allegations was deemed in advance to be unacceptable. The result of the investigation that actually took place was to identify two

individuals who had been working together for the previous 10 years to solicit and accept kickbacks.

Had the forensic accounting investigators confronted the targets early on as suggested by the division manager, it is unlikely that either would have confessed to the scheme. The strategic disadvantage of confronting the targets before substantive investigative work had been completed would have been too great a cost to pay for an unlikely event: their immediate confession. Admission-seeking interviews conducted in circumstances like these, without the benefit of facts discovered in a preliminary investigation, often put interviewers essentially in the weak position of simply taking notes. As to the division manager's suggestion that the forensic accounting investigators should have conducted an interview by telephone, the suggestion is easily dismissed as the least desirable alternative: Forensic accounting investigation is a field in which you should definitely not "let your fingers do the walking."

Confrontation is often the first thought that comes to mind upon encountering disturbing facts. Most people want to resolve matters immediately to allay their discomfort and get on with their own work. Unsettled and unresolved situations often cause disruption in organizations—never a good thing. Yet it is often better to go against natural impulse. An executive with suspicions should be advised to move carefully. There is often a tremendous strategic advantage when only one party—honest management—knows that an investigation is under way.

To sum up, admission-seeking interviews are often best conducted after learning certain facts through investigation. Facts are extremely useful in achieving investigative objectives; they are the friends of the honest person and the enemies of the fraudster. We recommend performing at least a preliminary investigation before interviewing the target. You may then be ready, at a relatively early stage of investigation, to test the veracity of a key individual. Should the individual admit wrongdoing or provide clear and persuasive evidence of honesty, procedures from that point forward may be brief and inexpensive. Do not confront the target until the appropriate preparatory work is completed. Sometimes a company employee begins to unexpectedly confess to wrongdoings to an executive or auditor. In such situations, it usually makes sense for the executive to continue talking with the individual. It would not be prudent to say to the subject, "Please hold that thought until I go get a forensic accounting investigator." These situations are rare, but they do occur. When the situation permits consideration of alternative approaches, enlisting the assistance of a forensic accounting investigator is often beneficial. Admission-seeking interviews are explored in Chapter 16, "The Art of the Interview."

DISMISSING THE TARGET

From the standpoint of a forensic investigation, an unfortunate fact that one might hear during the first call from an executive who believes that a fraud has been perpetrated on the company resembles the following: "We believe the controller has been recording bogus journal entries to inflate revenue. The evidence we have is quite solid, and we have just terminated him. Not surprisingly, he denied the allegations, but his denials carried no weight in light of the evidence we have on him. He's gone. Now we want to hire you to perform an investigation." From an investigative point of view, such a termination will often hamper an investigation.

Whenever there is a suspected defalcation, management and the board want answers to the following questions:

- Who is involved?
- Could there be co-conspirators?
- How much was stolen or what is the total impact on the financial statements?
- Over what period of time did this occur?
- Have we identified all material schemes?
- How did this happen?
- How was it identified, and could it have been detected earlier?
- What can be done to deter a recurrence?

Paid administrative leave may be less disruptive to an investigation than termination. The concerned executives are, naturally, angry over what they have found, but it is best to set anger aside for the duration of the investigation.

ASSUMPTIONS

Most auditors and their clients are intelligent people who have risen to positions of responsibility. Yet one of the features of high intelligence can be a detriment to investigation: Many smart people do not like to ask stupid questions. They prefer to think they can understand almost any set of circumstances by extrapolating intelligently on the basis of limited information. It follows that most intelligent people *assume* certain facts based on learned facts. Their assumptions may actually prove to be correct, but sound investigative conclusions cannot be based on assumptions. Whoever wrote the scripts for the long-running television shows *Columbo* and *Monk* understood a great deal about the conduct of a real investigation. Both characters appear to be bumbling, preoccupied, and confused. "Just one more question, ma'am: I'm really sorry to trouble you, but I forgot something that may be important." Now, most intelligent people are not like Columbo or Monk. Rather than ask an embarrassingly dumb question, they just assume a fact. This is unwise. It is far better to ask the simple question than to assume.

A good forensic accounting investigator is not an opiner but a fact finder. To do the job well does not mean the fact finder will make no assumptions whatsoever; rather, the fact finder will be strict about avoiding *needless* assumptions. Some assumptions are almost always necessary, but they should be made only when additional fact-finding is impractical.

Facts are so valuable to the forensic accounting investigator—and ultimately, to the trier of fact—because they provoke admissions and remove defenses the target could later use. Admissions include more than simply the target's direct admission of guilt. They encompass varied elements of evidence that can build toward concluding the matter at hand. In well-structured target interviews, those interviewed will make helpful admissions along the way, although they're unaware they're providing damaging information. Failing to see the whole picture, they realize they must cooperate with the investigation because lack of cooperation could suggest fraud—the last thing perpetrators want to suggest. For that reason, they're likely to give the

forensic accounting investigator bits and pieces of information, some of which could fit into a pattern that will eventually lead to clear and certain facts.

An illustrative example will help. Suppose it is important to a case to establish that the target knew the policy related to the authorization of certain expenses. It is also important to the forensic accounting investigator to understand exactly what the target has done with respect to approving and generating payments. The line of questioning proceeds as follows:

Q: How long have you been with the company and in this department?

A: Ten years with the company, three of them as director of accounts payable.

Q: What are the job responsibilities of the director of accounts payable?

A: [He explains all of his job responsibilities and indicates that he and he alone has primary approval authority for the validity of vendors and all payments to them.]

Q: What is your understanding regarding the required documentation for purchases of IT [information technology] consulting services?

A: I understand that any such services must be approved first by the IT department head and then by me.

Q: Is that for all services, or is there some dollar limitation?

A: It is for all purchases greater than $5,000.

Q: So then, purchases of $5,000 or less do not need approval by the IT department head—only your approval. Do I have that right?

A: Yes.

Q: I just want to be certain I know what your sign-off or initials look like. Is this it? [The interviewer places in front of the target a copy of the initials reproduced from some of the fraudulent approval documents. The target is not aware that his initials were copied from such documents.]

A: Yes, that's my sign-off.

Q: Besides you, are there any others in your department or another department who could approve such transactions without your knowledge?

A: No.

Q: Are you certain?

A: Yes.

Q: And if you're on a business trip or taking a vacation?

A: We're a small shop. They wait for me to return. I travel infrequently, and my vacations never extend longer than a week. The vendor can wait.

Q: Have there been instances in the past three years when this practice has not been followed?

A: No.

Q: You seem sure of this.

A: I know my department and company policy, and I run a tight ship.

Let's review the circumstances and then look at what we have learned through this interview. First, the premise for the interview: Although the target does not know

it, forensic accounting investigators have found 28 checks of less than $5,000 each that were written during the past three years to a legitimate vendor of the company. They have established that an individual at the vendor company is a co-conspirator and that the invoices issued by the co-conspirator were for nonexistent services. They also have a number of checks significantly higher than the $5,000 limit, which they suspect are for nonexistent services, but they're not yet sure of their facts. Their best strategy is to induce the target to admit the fraud involving checks of less than $5,000 and then work their way toward finding out that others are involved in a scheme to defraud the company on much larger purchases of IT consulting services.

One of the target's defenses may be that he was unaware of a fraud and simply approved payment of the invoices in accordance with company policy. In actuality, as the forensic accounting team later discovered, there was a trio of conspirators, including the company director of accounts payable—our target interviewee—a company department head, and an individual at the vendor company. All of the suspicious checks, when received by the vendor, were endorsed with just a checking account number and no company name and were deposited into an account other than the target's primary checking account, known from his payroll direct deposit.

Prior to the interview with the target, the forensic accounting team strongly suspected he had stolen money; they were not blindly confronting the accounts payable manager, he had not been fired, and they were keeping their assumptions to a strict minimum. However, there was much they did not know: They did not know quite how the target did it, how long he had been doing it, whether there were co-conspirators, and whether this was the only scheme he used. Because the accounts payable manager knew the forensic accounting team was investigating, he was unlikely to perpetrate additional thefts until they left the scene.

Let us now examine what the investigative team knows because it did not assume facts but instead chose to ask a great many seemingly dull, repetitive, and unnecessary questions. The team is certain of the following:

- From investigation before the interview, the team knows that through this scheme alone—there may be others as yet undiscovered—the target stole about $625,000 in the past three years.
- By his own admission, he is the sole approver on transactions of $5,000 or less.
- By his own admission, no one else could have generated the checks without his knowledge. He either knew or should have known.

As you will learn from the later admission-seeking interview of this target in Chapter 16, he admitted to the theft and disclosed important facts of which the investigative team had been unaware. All of this occurred because the forensic accounting team structured the interviews in such a way that the target was left with no escape hatch.

Had they *assumed* facts and had they then been wrong in their assumptions, here is how the target could have evaded the truth when confronted. Assume that the line of questioning proceeded in roughly the following way:

Q: How long have you been with the company and in this department?

A: Ten years with the company, three of them as director of accounts payable.

Note: The interviewer assumes he knows what a director of accounts payable does and therefore does not seek clarification from the target. This is an error. We record in this box, and in boxes to follow, the critical gaps in the interview.

Q: What are the job responsibilities of the director of accounts payable?

Q: What is your understanding regarding the required documentation for purchases of IT consulting services?

A: I understand that any such services must be approved first by the IT department head and then by me.

Q: Is that for all services, or is there some dollar limitation?

A: It is for all purchases greater than $5,000.

Q: So then, purchases of $5,000 or less do not need approval by the IT department head—only your approval. Do I have that right?

A: Yes.

Note: The interviewer feels he does not need to confirm the target's sign-off. He's seen it many times and therefore takes a pass on this question—a decision he will come to regret.

Q: I just want to be certain I know what your sign-off or initials look like. Is this it? [The interviewer places in front of the target a copy of the initials on some of the fraudulent checks. The target is not aware that his initials were copied from such documents.]

Q: Besides you, are there any others in your department or another department who could approve such transactions without your knowledge?

A: No.

Later, the interviewer calls on the target for what he believes will be an admission-seeking interview. The interviewer lays out some of the fraudulent canceled checks and invoices with the target's initials signifying approval. The interviewer tells the target that he believes the target knew these invoices were for services not performed and that the target benefited from the scheme. The target looks at the interviewer in shock and amazement and immediately denies the allegations. Undeterred, the interviewer then confidently discloses more evidence.

Q: You told me previously that you are the director of accounts payable. You should have known about this.

A: Sure, that's my title, but our controls are not as tight as they should be around here. Others could have put my initials on that invoice.

Q: Are you telling me that is not your sign-off on this invoice?

A: That's exactly what I'm telling you.

Note: Now he has the interviewer on the defensive. The interviewer assumed that as director of accounts payable, the target controlled everything in his department. He also assumed that the invoice contained the target's sign-off.

Q: You told me that you and you alone approved transactions of this type.

A: That's not true; I must have misunderstood your question. When I'm not here, others can approve these types of transactions. We're pretty loose around here because we're a small shop. All I can tell you is that those are not my initials.

Note: Now the interviewer is frustrated, while the target is doing a fine job of wiggling out of the accusations. The interviewer's case theory and proof are disappearing. Taking a closer look at the invoices and comparing the target's initials with the initials on the invoice, the interviewer sees that they arguably show some degree of dissimilarity. Beginning to doubt his own case, the interviewer decides on the spot not to move on to the matter of conspiracy with others to falsify even larger payments. The initial confrontation with the target has failed. It has failed because of too many assumptions and too few verified facts.

THE SMALL STUFF COULD BE IMPORTANT

For the most part, auditors devote much of their time to auditing material transactions and account balances, and many such tests are directed at balance sheet items and accounts. With the exception of revenue and certain expenses with unique risk, a fair portion of time allocated to the auditing of accounts such as selling, general, and administrative expenses (SG&A) on the income statement focuses on the adequacy of controls as opposed to individual transactions. That focus is for many reasons, not least among them what the profession calls *detection risk*: The risk that a material misstatement will occur and not be detected by planned audit procedures is generally greater in respect of material transactions and account balances than in respect of individually small expense payments. Furthermore, keep in mind that if a significant amount of money gets embezzled but the theft is run through the income statement instead of being hidden on the balance sheet, the fraudster is taking advantage of general perceptions of detection risk to more effectively hide the scheme. This is a technical point, but a simple example can clarify it.

The theft of $2 million is a substantial loss, but in the context of detection of material misstatements at a company with $30 billion in total assets and $18 billion

in SG&A (assume that the fraud is buried under this caption), $2 million is likely to be quantitatively immaterial to the financial statement taken as a whole. Even if pretax net income is only $1 million (net of the fraud for purposes of this example), it is included in SG&A and therefore in the determination of net income. Of course, qualitatively, the financial statements contain a misstatement in that funds that were actually stolen have been characterized and reported as a productive expenditure of the company. Both qualitative and quantitative materiality have to be evaluated according to relevant professional standards before determining whether the financial statements taken as a whole are, or are not, materially misstated, but regardless of that conclusion, because the theft is already recognized in the determination of net income—along with many other individually small transactions—it is more difficult to detect.

The difficulty in detecting such embezzlement schemes is somewhat different if the $2 million were recorded on the balance sheet as a hanging debit[2] in accrued expenses or accounts payable. Quantitatively, however, the $2 million theft (presumably recorded as some sort of asset or as a reduction to a liability) would be material when detected and written off in comparison to the company's pretax net income. Continuing with the example, because it does not flow through the income statement, the $2 million write-off would now be considered relative to $3 million in pretax net income and by most quantitative assessments would be material to net income. Since management, internal auditors, and external auditors all give substantial consideration to balance sheet errors that could be material to reported net income, the chance that this $2 million hanging debit will be detected and dealt with is increased. There have been several examples in which a fraudster took advantage of knowledge of the auditor's detection risk and quantitative materiality assessments to hide a theft by running it through the income statement, including breaking up the transactions among a few hundred expense accounts.

In both scenarios, the fraud is hidden until discovered, but in one the fraudster uses knowledge of risk and quantitative materiality assessments to more effectively shield the scheme from discovery. If the theft is concealed in SG&A, detection is more difficult for the company and its auditing firm in part because of the quantitative aspects of detection risk and materiality judgments—even though both would very much like to know about such a defalcation. A company needs to determine whether a theft of this amount represents an acceptable detection risk. If not, it can design appropriate controls to mitigate the risk. Even frauds that do not rise to a quantitative level of financial statement materiality could prove to be embarrassing. Defalcations, whether material or not by the standards of generally accepted accounting principles, reduce a company's value. Accordingly, some companies, through their internal audit group, design audit tests to mitigate the risk that such frauds can occur and go undetected. Such tests involve procedures that go beyond the audit procedures commonly selected by internal and external auditors alike. Among the more advanced

[2] A hanging debit is a charge that should have been recorded on the income statement but is placed on the balance sheet instead. Whether recorded in error or with the intent to deceive, the charge is inappropriate. A hanging debit is similar to a suspense account, with the key difference being that a hanging debit is hidden in a standard balance sheet account, such as accounts payable—usually with the intent to hide it from discovery.

and more thorough techniques, data mining can be particularly helpful in detecting such frauds (see Chapter 17).

MATERIALITY: MORE ON A KEY TOPIC

Auditors live in a world in which materiality matters. While auditors, management, investors, and other constituents and members of the corporate-reporting supply chain would prefer that all frauds be exposed, that is not a realistic objective, because most fraud is immaterial to the financial statements taken as a whole. On one hand, the financial burden of audits designed to uncover all frauds of any size would be unimaginably onerous. On the other hand, the public and the capital markets want independent and searching checks of the books and records of public companies. Not surprisingly, the audits of today fall somewhere between the two extremes. Herein lie the questions: How much auditing is enough? And when is it prudent to pursue a matter even if it is immaterial?

Before the Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit* (SAS 99), many errors in record keeping were dismissed because they fell below the materiality threshold established by the auditing firm at the outset of the audit. *Pass* or *waive due to immateriality* were and remain legitimate expressions in the auditor's working papers, signifying either a transaction, groups of transactions, or balances that had been noted but that fell below the predetermined threshold. Subsequent to SAS 99, though, specifically as required by paragraphs 75 and 76, the auditor can no longer dismiss all such immaterial occurrences at first sight without further consideration. The two paragraphs read, in part:

> 75. Responding to misstatements that may be the result of fraud. *When audit test results identify misstatements in the financial statements, the auditor should consider whether such misstatements may be indicative of fraud. That determination affects the auditor's evaluation of materiality and the related responses necessary as a result of that evaluation.*
> 76. *If the auditor believes that misstatements are or may be the result of fraud,* but the effect of the misstatements is not material *to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the person(s) involved* [emphasis added]. *For example, fraud involving misappropriations of cash from a small petty cash fund normally would be of little significance to the auditor in assessing the risk of material misstatement due to fraud because both the manner of operating the fund and its size would tend to establish a limit on the amount of potential loss, and the custodianship of such funds normally is entrusted to a nonmanagement employee. Conversely, if the matter involves higher-level management, even though the amount itself is not material to the financial statements, it may be indicative of a more pervasive problem, for example, implications about the integrity of management.*

While to some these requirements may seem in many respects exercises in chasing rainbows, they actually often represent excellent fraud detection practices. The loose-thread theory, discussed in Chapter 11, suggests that most fraud is very difficult to

detect and that, once indicators are found, it is risky to ignore loose threads. The loose thread could be an indicator of a large fraud. Under the new auditing guidance, the auditor is instructed to "evaluate the implications" of the transaction, especially with regard to the position of the culpable party. If an accounts payable clerk wrote a check to himself for $30,000, it may be an immaterial event. However, if the culpable party was the divisional controller, you have quite a different matter on your hands. If the controller did this much, what else could that controller have done? This is when the forensic accounting investigator could provide useful assistance by, for example, looking at everything the controller touched. This may assist an assessment as to the overall possible effect on the financial statements.

ADDRESSING ALLEGATIONS

Even though the False Claims Act, which gave birth to the modern-day whistle-blower, has its roots in legislation that dates back to the Civil War, society has historically frowned upon snitches. With the increase in corporate ethics programs, training, and education, that historically held negative attitude has given way to a broadly shared employee awareness of corporate responsibility to come forward and "do the right thing." In fact, three whistle-blowers were selected for person-of-the-year honors by *Time* magazine in 2003. Employees are now held to a higher standard of integrity in the workplace, a standard that approaches military values and discipline. For example, the honor code at the Virginia Military Institute in Lexington, Virginia, is inscribed on the front wall of every classroom. It reads, "A Cadet will not lie, cheat or steal, nor tolerate those who do." The refusal to accept others who do has moved a long way toward becoming an expected element in the code of conduct in many corporations.

There is always some initial skepticism as to the credibility of a whistle-blower allegation. Thoughts of grudges against the company or against certain individuals or a failure to understand the legitimacy of an unusual business transaction may come to mind as the person responsible for the hotline or whistle-blower communications takes a first look at allegations. It is actually quite natural to discount calls or letters that offer sketchy details, at best, about an alleged illegal or unethical act. However, the best advice is to investigate all such letters and calls. The extent of the investigation is a matter of professional judgment, with all appropriate parties weighing in on that decision. It is important to be mindful of the reporting requirements regarding such letters and calls under the Sarbanes-Oxley Act.

Apply the loose-thread theory to these types of allegations. On one hand, if anonymous allegations are not properly investigated, no harm may be done and the communication may be no more than a shot in the dark from someone with a grudge. On the other hand, there are two more possibilities. First, the allegation could be true. If you ignore it, the fraud may continue and the whistle-blower may return to daily duties with the conviction that the company does not care even about its own assets, let alone its employees. Or, the whistle-blower may persist in seeing that justice is done—for example, by making contact with the U.S. Securities and Exchange Commission (SEC) or the U.S. Department of Justice, expecting to find a more receptive ear. No one wants to begin the day with a call from an assistant

U.S. attorney announcing that both the company and the chief financial officer are targets of investigation.

THE CASE OF THE CENTRAL AMERICAN GENERAL MANAGER

Many of the potential missteps discussed earlier are addressed in the following case study. As fully as any narrative in this book, the case illustrates that a forensic accounting investigation is a complex process, thoroughly distinct from financial auditing, although using some of the auditor's methodologies.

The divisional controller of a $500 million Central American food processing unit of a Fortune 500 company received an anonymous letter alleging several important but relatively minor offenses. The letter alleged that the general manager (GM), whom we'll call John, was cheating on his expense reports, using company property for personal use, and having an affair with his secretary. The controller—let's call him Paul—could have been inclined to discount the allegations, as John had been honored at the most recent global meeting as a role model for other GMs. An expatriate from Michigan with a PhD in chemical engineering, John had been with the company for 22 years.

On the few occasions when Paul had met John, he was impressed in every way. Why should he be overly concerned, even with this anonymous letter in front of him? It could be from a disgruntled employee. However, Paul had learned long ago that things are not always what they seem. The letter was a potential red flag, and he preferred not to dismiss it until properly investigated. Some years earlier, Paul had encountered another "John" and elected to ignore certain trouble signs, only to learn later that the suspect in that instance was defrauding the company. Since then, Paul had learned to take all such indicators seriously. Trust but verify.

Paul first dispatched three internal auditors to interview John and several other executives and to poke around to see whether anything surfaced. The team spent a week on the task and reported that all seemed to be in order. Nonetheless, Paul decided to wait until the external auditors finished their statutory audit, due to begin in a few weeks. In the course of that audit, the auditors showed the letter of allegations to John and recorded his responses. John flatly denied the allegations and invited what he called a full audit to clear his name. When asked why someone would be motivated to send such a letter, he said that recent, necessary changes in overtime policy might have angered an employee.

Chapter 16 addresses the art of interviewing and surveys the most effective means of obtaining answers to sensitive and critical questions without asking the obvious questions for which the target will almost certainly have well-prepared answers. In this case, if the auditors felt compelled by the statutory requirements of their profession to question John about the allegations, they might have been more effective had they used some of these strategic techniques.

It might have been strategically wiser to approach him in something like the following manner: "John, as a part of our review, we'll be questioning employees, including your secretary, about their comfort level with the integrity of management at this plant. Can you forecast what their responses might be?" If John has been acting with integrity, he would likely answer without hesitation, "All is appropriate, and I don't know why anyone would think otherwise." However, if he has been

engaging in inappropriate activities, he might pause before responding and may have a troubled look on his face. He'll have to construct a story that allows for the possibility of someone's coming forward to reveal his illicit deeds—perhaps his secretary. If he is in fact guilty of wrongdoing, he may go so far as to provide the auditors with anticipatory reasons why some may attempt to implicate him. On the forensic accounting investigator's part, at this point, silence is golden. It may cause the target to feel uncomfortable or offer a rambling response that points in a certain direction. Remain silent, wait for the subject to answer as completely as he wishes, be attentive, take good notes.

The auditors completed their statutory audit and reported to Paul that the allegations seemed without basis. They had found nothing to indicate wrongdoing, although they had even confronted John with the letter. Paul, however, remained unsure. He decided to contact the engagement partner from the external audit firm, who until now knew nothing of the possible problem. "Do you have a forensic accounting group? I'd like to talk to them." Acting quickly, the audit partner called in forensic accounting investigators.

The forensic accounting investigators now engaged in this investigation knew that they should not immediately confront John with the allegations put forth in the letter. The lead forensic accounting investigator chose to interview him in an attempt to determine whether he was an honorable person or had something to hide. Such an interview needs a factual basis to be effective, and so the forensic accounting investigator hired a private investigator to perform a weeklong investigation in John's hometown. Certain facts emerged. John owned a small office building in which he housed two businesses, the nature of which was not readily apparent. He also had a passion for classic boats. He owned 12 classic boats and was president of a local boating club with about 40 members and a lavishly appointed clubhouse. The forensic investigator wondered who had paid for the clubhouse. In any event, he now had an array of facts that could serve as a litmus test of John's truthfulness, and it was time to pay him a visit.

The forensic investigator received a very warm welcome from John in his office, which was surprisingly well appointed. Prominently placed on his desk was a framed advertisement of a well-known gun manufacturer displaying a variety of shotguns and automatic weapons. This was the first thing that caught the forensic accounting investigator's eye as he sat down, and he wondered whether this unusual "office art" was deliberately intended to send a subliminal message.

John began the substantive part of the meeting by informing his visitor that there had been a break-in at his offices just the night before. He inquired whether his guest was aware of local reports of civil unrest. Replying no, that he was not familiar with local matters, he redirected the discussion back to the break-in. John then reported that people who were believed to be disgruntled workers had stolen the window air conditioner in the accounting department and also "stolen all the accounting documents." He pointed out that further examination of accounts by the external auditor would be impossible from a historical perspective due to this wholly unfortunate turn of events.

The forensic accounting investigator remarked that he had noticed disarray and confusion in the accounting department as he was escorted to John's office. He added that the computers had not been stolen and were apparently undamaged. He offered to send in IT professionals to assist John's group in rebuilding the accounting

documents and expressed his willingness to return at a later date to review the accounting records. Surprisingly, John had not foreseen this set of possibilities. He paused for what seemed a long time, head down, until he reached what he felt would be an adequate response.

Here is an application of the use of silence in an interview. After the forensic accountant commented that his firm's IT team could assist in restoring the accounting records, he became silent. He did not care if John sat there, head down, pondering his response, for hours. He was not going to let him off the hook by offering any further options. He wanted to let John come up with his own story and was prepared to wait patiently for it. Silence and inactivity at the right moment also represent a good technique for assessing the veracity of a target's responses. How long does the individual pause? What are his facial expressions and physical movements during this period of doubt and stress?

After a minute or so had passed—an eternity in a free-flowing conversation—John responded: "That would not be possible. They also stole the computer hard drives." Now, the first reaction to this news might be a hearty laugh. "Sure," thought the forensic accounting investigator, "the individuals involved in the rumored civil unrest had brought along their Phillips screwdrivers, had stolen the hard drives, and at this very moment were installing them in their home office computers." In reality, most of the city was not equipped with either the electrical or communications infrastructure necessary to support widespread personal computer usage, but, playing along, the forensic accounting investigator quietly remarked that this recent turn of events did indeed present problems. He said he would be leaving the country the next day and would inform both his audit partners and the company's corporate headquarters that examination of the local accounting records was impossible at this time and that he would await their further counsel.

John and his guest then went to lunch. Believing he had completely fooled the forensic accounting investigator, John became relaxed and casual and the forensic accounting investigator found in this setting an opportunity to explore further John's truthfulness.

The treatment John received at the restaurant was impressive. He was obviously a regular—private room, an exclusive server, attention worthy of a dignitary. All of these were indications that John was an influential individual. As the forensic accounting investigator was later to learn, John had paid plenty for this kind of treatment. The lunch moved leisurely into its second hour, when the forensic accounting investigator felt that the time was right to pose certain questions to test John's integrity. "John, you're obviously a very successful businessman, and the company holds you in high regard. What do you do when you're not working so hard?" He was reaching out to see whether John would mention his side businesses and his passion for classic boats. John replied that he was devoted to the company and had no time for pleasures apart from an occasional trip to the United States or his native city. The forensic accounting investigator pushed the question in another form—in order to give John one more opportunity to be honest. He did not bite. He insisted that he had no time for simple pleasures. His job demanded his full and complete attention.

At the end of lunch, the forensic accounting investigator thanked John for his hospitality and expressed the hope that they would get together again soon. John left, thinking he had successfully concealed his deceitful operations and believing the

forensic accounting investigator would convey the message to corporate that John was an able manager, although certain unfortunate events had occurred owing to the break-in and would soon be rectified. In other words, John was relieved and confident, not suspicious, and thus unlikely to take any further steps to hide his fraud while the next phase of the investigation was being planned.

The forensic accounting investigator met two days later in the United States with the corporate management committee. He reported that although the size of the problem was unknown, he believed there was a problem.

Now let's dissect some of the features of this case that explain why the forensic accounting investigator came away with a different opinion from both the company's internal auditors and the external audit team. The internal and external auditors knew more about the target and the operations of his plant than the forensic investigator would ever know. However, the forensic accounting investigator applied the lessons of a long career in practical forensic investigation.

EXERCISING SKEPTICISM

Trust but verify: This was the guiding principle during the initial meeting with John. The forensic investigator knew he could not properly evaluate the interview or the evidence from the accounts, had there been any, if he allowed bias of any kind to affect his judgment. The forensic investigator's mind was completely open—free of assumptions about the individual's character or acts. However, after the initial interview, including the telling conversation at lunch, the forensic accounting investigator had collected enough facts to shift rapidly toward suspicion. The forensic accounting investigator walked away from John with the concern that if John had lied about the theft of accounting records and refused to disclose his passion for classic boats and his other business operations, he was perhaps concealing other matters of greater importance. There was, as yet, no evidence of fraud—but there was compelling basis for believing the investigation should continue.

This forensic accounting investigator understood how to conduct the investigation, including the nature, extent, and timing of investigative procedures and who should perform them. Performing the correct procedures at every turn, the forensic accounting investigator was methodical in the application of those procedures and in the evaluation of evidence. The result or conclusion from such an investigation is simply a culmination of all of the facts uncovered, together with a minimum of assumptions when facts are still missing. If all the facts fit a pattern of fraud—either a fraud known from prior investigations or a new twist on an old theme—the forensic accounting investigator can be *reasonably certain* that the target with or without co-conspirators has perpetrated a fraud.

This is not to apply the familiar criminal standard of guilt beyond a reasonable doubt. As discussed in Chapter 20 and elsewhere, proving fraud to the beyond-a-reasonable-doubt criminal standard may ask too much of a company before it moves to cut its losses by suspending or firing the alleged fraudster or turning over evidence to the appropriate law enforcement agency. A judge or jury as the trier of fact may ultimately make a determination that the evidence, both circumstantial and testimonial, meets the standards for criminal conviction. This is not the forensic accounting investigator's assignment. Forensic accounting investigators are fact finders.

CASE OUTCOMES

In this chapter of potential missteps, the case study investigating John's deceptions has illustrated sound practices. What happened to John? There is good and bad news. The ensuing investigation, covering a span of 12 weeks, was arduous because of John's tactics of intimidating employees and refusing to provide requested documents. It did not take long for him to realize he was the central target of investigation, and he played every angle to dissuade the forensic accounting team from doing its job and to prevent his employees from talking. In the end, the investigation determined that he had embezzled $35 million over a period of two years. Most of it was hidden on the balance sheet in the intercompany account and had hanging debits in accounts payable. The approximately $2 million that did flow through the income statement was buried in the foreign currency translation account to take advantage of the country's high currency fluctuations. That explanation was given to the audit firm and recorded in its "reasonableness" test working papers for this expense account.

The company terminated John, 15 of his managers and supervisors, and the president of that division in the United States. Within the next two years, the company also closed the plant for which John had been responsible.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 13

Potential Red Flags and Fraud Detection Techniques

Will Kenyon and Patricia D. Tilton

As noted in earlier chapters, management is responsible for the quality of financial statements and an organization's internal control structure. Statement of Auditing Standards (SAS) No. 1 states this: "Management is responsible for adopting sound accounting policies and for establishing and maintaining internal control that will initiate, record, process, and report transactions consistent with management's assertions embodied in the financial statements." Sections 302 and 404 of the Sarbanes-Oxley Act of 2002 require certifications by members of management as to the completeness and accuracy of financial reports and the nature and effectiveness of internal controls. Management is also responsible for establishing and maintaining proper compliance systems, which is beginning to be reflected in regulatory initiatives in the enforcement and legislative communities of both the United Kingdom and the United States.

The accounting literature about the auditor's role in fraud detection is extensive. At its core it states, "The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud." SAS 99 and AU Section 316, *Consideration of Fraud in a Financial Statement Audit,* are the current standards on this topic and are discussed throughout this chapter. Related guidance includes SAS 54, regarding illegal acts (partially superseded and partially supplemented by SAS 82, which was superseded by SAS 99), and SAS Nos. 60 and 71, addressing reportable conditions related to internal control defects. Other relevant guidance includes SAS 22 (planning and supervision), SAS 31 (evidential matter), SAS 47 (audit risk and materiality), SAS 56 (analytic procedures), SAS 57 (accounting estimates), and Public Company Accounting Oversight Board (PCAOB) Auditing Standard 2 (AS2). Also, the report by the Treadway Commission's Committee of Sponsoring Organizations (COSO) provides a framework for internal control that forms the basis for the rules of the PCAOB.[1]

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework* (New York: COSO, 1994).

Federal legislation also addresses the issue of auditor responsibility. Title III of the Private Securities Litigation Reform Act of 1995 indicates that each audit shall include procedures designed to provide reasonable assurance of (1) detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts and (2) detecting material related-party transactions. Sarbanes-Oxley requires that auditors attest to management's report regarding internal controls and procedures for financial reporting.

This chapter discusses potential red flags and available detection techniques for fraud schemes.

TYPES OF FRAUD REVISITED

Fraud schemes can be frauds *by* the corporation or frauds *against* the corporation. Frauds committed by the corporation carry legal risk—potentially civil, regulatory, and criminal in nature. Frauds committed against the corporation carry the risk of loss of income or assets for the corporation—and the risk of discovery and prosecution for the perpetrator.

This chapter and those that follow consider four broad categories of fraud that may significantly affect financial statements. They are:

1. Fraudulent financial reporting schemes
2. Misappropriation of assets—by far the most common fraud against the corporation
3. Revenues and assets obtained by fraud
4. Expenditures and liabilities for an improper purpose

SAS 99 instructs auditors to focus on two areas of fraud—fraudulent financial reporting schemes and misappropriation of assets—each of them encompassing many other types of schemes. We will be more concerned here with these two types of fraud than with the second pair in the preceding list, although these, too, can be significant. Corruption—the use of official authority for private gain—straddles all of these categories. Corruption in the traditional sense generally involves government officials' profiting from their public office (see Chapter 26). What might be thought of as private corruption—a breach of fiduciary duty—also exists; for example, corporate officers' abusing their authority for personal gain. The recipients must obtain a gain without the knowledge or consent of their employer and in contradiction to their duty of loyalty to their employer. The most common corruption mechanisms are bribes and kickbacks. Bribes are *paid*; kickbacks are *received*. While it may appear that the entity involved is unharmed by the illegal payment to its employee, ultimately, most kickback schemes result in overbillings to an entity. The frequency and severity of corruption in the business community and in public affairs varies widely by nation and in some cases by industry. Based on global surveys of corruption and economic crime, it is safe to say that no industry or country is immune to this issue.[2]

[2] Transparency International Corruption Perception Index 2009, www.transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table; PricewaterhouseCoopers, *Global*

It is costly and is among the hardest schemes to detect because it is typically off the books. (See Chapters 22 and 23 on common fraudulent schemes.)

Financial reporting fraud, as previously noted, can be *inclusive,* meaning that false entries are made to the company's books and records, or it can be *exclusive,* meaning that entries required for the fair presentation of financial statements are omitted. In either case, fraud is distinguished from error by the intent of the action. Fraudulent misstatements, often perpetrated by managers, include such acts as manipulation or falsification of financial or accounting records, like recording fictitious sales; financial statement misrepresentation of events or transactions, like incorrect inventory valuation; and intentional misapplication of accounting principles with respect to amounts, classification, and manner of presentation or disclosure, like a classification of short-term debt as long-term debt or refraining from disclosing a contingency that may represent future losses for the company.

In addition to financial statement frauds, auditors are concerned with frauds involving material misappropriation of assets. Asset misappropriation is by far the most common type of fraud,[3] although the size of the loss from an individual asset misappropriation scheme is typically smaller than that from other fraud schemes.[4] Misappropriation of assets involves theft of an entity's assets. These acts usually involve one or more individuals among management, employees, or third parties. Misstatements occur when the effect of the theft causes the financial statements not to be presented in conformity with generally accepted accounting principles or when adjustments are intentionally made to hide the theft. Misappropriation of assets can be accomplished in various ways—for example, stealing assets such as cash or inventory or making an entity pay for goods or services it did not receive (in other words, fraudulent disbursements).

FRAUD DETECTION: OVERVIEW

Detecting fraud is difficult, especially frauds involving material financial statement misstatements, which occur in only about 2 percent of all financial statements. Fraud is generally concealed and often occurs through collusion. Normally, the documents supporting omitted transactions are not kept in company files. False documentation is often created or legitimate documents are altered to support fictitious transactions. While fraud detection techniques will not identify all fraud, the use of sound

---

Economic Crime Survey 2009, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf; PricewaterhouseCoopers, *Global Economic Crime Survey 2007*, www.pwc.com/en_GX/gx/economic-crime-survey/pdf/pwc_2007gecs.pdf.

[3] PricewaterhouseCoopers, *Global Economic Crime Survey 2003,* 7, which cites this fraud at an incidence rate of approximately 60 percent.

[4] Association of Certified Fraud Examiners, *2002 Report to the Nation on Occupational Fraud and Abuse* (Austin, TX: Association of Certified Fraud Examiners, 2002). Based on survey responses from 663 certified fraud examiners: 85.7 percent of fraud schemes involved asset misappropriation, 12.8 percent involved corruption, and 5.1 percent involved fraudulent financial statements. (The total percentage exceeds 100 because some of the fraud involved more than one scheme.) The median losses, respectively, were $80000, $530000, and $4.25 million.

techniques can increase the likelihood that misstatements or defalcations will be discovered on a timely basis.

Knowing where to look is the first step in fraud detection. Understanding the motivations of those committing fraud and knowing in which accounts fraud is more likely to exist based on a risk assessment helps identify the areas that might be subject to greatest scrutiny. Similarly, being aware of the types of transactions that warrant further review, as well as other potential red flag indicators, may alert auditors to areas that might require a closer look. Specific detection techniques discussed in this chapter include carrying out analytic procedures, using unpredictable audit tests, observing and inspecting, making inquiries, and conducting interviews. While these techniques may be performed routinely in the course of a financial statement audit, approaching them with the mind-set of professional skepticism (Chapter 11) and with better knowledge of the various types of fraudulent schemes (Chapters 22 and 23) may make the difference between detecting and not detecting fraud. This chapter also discusses the importance of continually bringing together all of the information obtained through the application of these detection techniques and evaluating the risk of fraud on the basis of such information.

The detection techniques discussed in this chapter—including techniques performed as a routine part of audits—rely on certain procedures and attitudes to achieve the desired result of detecting fraud. These key procedures and attitudes include the following:

- Perform all procedures with an attitude of professional skepticism.
- Consider deception techniques during the review of documents, including the possibility of falsified documents.
- Thoroughly understand and be alert to potential red flags that are possible indicators of irregularities and likely indicators of areas requiring further analysis.
- Request more documentation in fulfilling audit responsibilities.

In summation, trust but verify.

Most audits do not result in the detection of material misstatements from fraud by management or others, for the simple reason that most audited financial statements are free of such misstatements. On the face of it, this is good news and it is important not to lose sight of this fact in any discussion of fraud risk. But the fact that material misstatements due to fraud are relatively rare does not diminish the grave consequences for companies, auditors, and stakeholders when such cases arise. No one in the corporate reporting chain can become complacent about the honesty and integrity of management.

When a material misstatement due to fraud arises, the actions or omissions that give rise to the misstatement often occur over an extended period. The initial financial accounting impact may be relatively insignificant but can accumulate over time. Management may seek, for example, to mask a revenue shortfall in one period by accelerating recognition of certain transactions that belong in the subsequent period. The impact at the initial stage may not be material, and the intention may not be consciously fraudulent.

Management may have persuaded itself—that is, may have rationalized—that its actions are justified to smooth over a short-term dip in sales and that the long-term effect will be negligible when business recovers. Should business fail to pick up in the

next period, however, management is faced with a double problem: It has contributed to unrealistic revenue expectations, and the shortfall is now compounded by the fact that revenues that should have been booked in the current period were recognized in the previous period. Should management choose to persevere in plugging the gap, it may need to be even more aggressive in its revenue recognition—to the extent that at some point it may create fictitious transactions to make the numbers.

The challenge for the auditor is to recognize early any signs that a material misstatement may have occurred or might occur if the same policies and practices are continued. SAS 99[5] envisages a series of steps, as follows, which are designed to assist the auditor in identifying, evaluating, and responding to the risk of material misstatement due to fraud:

- Holding discussions among the audit team concerning fraud risk
- Obtaining information relevant to the identification of fraud risk
- Identifying the risk of material misstatement due to fraud
- Assessing the identified risks, taking into account the internal controls designed to address those risks
- Responding to the results of the assessment
- Evaluating audit evidence

We will look at each of these steps in turn.

While SAS 99 presents the approach of identifying and addressing fraud risk factors as a series of discrete and sequential steps, the reality is likely to be more fluid. The collation and interpretation of evidence that may indicate the presence of fraud risk factors require a holistic, iterative approach that is unlikely to be achieved simply by adhering to a set of procedures or applying a checklist. The steps set out in SAS 99 are a means to an end, not an end in themselves. This holistic, iterative approach is reflected in SAS 99; for example, paragraph 75 instructs the auditor to consider whether audit test results identifying misstatements may be indicative of fraud. SAS 99, paragraph 76, expands on that requirement.

If the auditor believes that misstatements are or may be the result of fraud but the effect of the misstatements is not material to the financial statements, then the auditor nevertheless should evaluate the implications, especially those dealing with the organizational position of the persons involved.[6]

There are two reasons for this. First, even immaterial frauds can prove embarrassing to the company and the auditor, thereby diminishing investor confidence in

---

[5] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), October 2002. SAS 99 supersedes SAS 82 (having the same title) and is applicable to all audits required to be conducted in accordance with U.S. Generally Accepted Auditing Standards (GAAS) and is effective for audits of financial statements for periods beginning on or after December 15, 2002. Readers based outside the United States will want to know that International Standard on Auditing (ISA) 240, "The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements," issued by the International Auditing and Assurance Standards Board of the International Federation of Accountants, may be applicable.

[6] Id., pars. 75, 76.

the quality of the audit and the reliability of management's representations. Also, frauds often occur gradually, starting small and growing over time. Finding a small fraud may be the window to an even larger one not yet discovered. (See the discussion of the loose-thread theory in Chapter 11.)

The discovery of material misstatements in a set of financial statements, resulting from deliberate acts or omissions on the part of management or others, commonly prompts questions as to how such a situation could have arisen, whether it could have been discovered sooner, and if so, why it was not. With hindsight, it is all too easy to see facts and circumstances that, had they been identified earlier and interpreted differently, might have enabled the auditor to uncover the fraud and make appropriate disclosure.

The attempt to convert some of this hindsight into foresight has become an increasing focus of auditors, standard setters, and regulators alike. Their approach is to try to distill from past experience those events or circumstances related to any business, its management, and its environment that are commonly associated in one way or another with fraudulent acts or omissions. These are referred to as fraud risk factors or, more informally, potential red flags.

LAYING A FOUNDATION FOR DETECTION

An auditor's ability to detect fraud may be significantly enhanced by personal understanding of an enterprise and the environment in which it operates. With this knowledge, the auditor may be better able to identify anomalies or other potential red flags such as nonsensical analytic relationships, control weaknesses, transactions that have no apparent business purpose, related parties, and unexpected financial performance. It is important to understand the business, the control procedures in place, the budgeting process, the accounting policies, the industry, and the general economic climate affecting the company.

To understand the business, and how it makes money, it is important to identify the key business partners (customers, vendors, and so forth) and understand the corporate culture and organizational structure. To understand the industry, auditors might identify competitors or comparable companies, determine how the competitors and comparable companies perform, and consider changes in the competitive structure such as mergers and new entrants to the market, changes in the company's market share, and trends and overall issues affecting the industry. SAS 22 offers additional guidance on obtaining knowledge about an entity's business and its relevant industry. Such information provides a critical foundation for the evaluation of the information obtained through the techniques discussed later.

Assessing the Risk of Fraud

Some level of uncertainty and risk exists in any financial statement audit. For example, there may be uncertainty about the competence of management and the accounting staff, about the effectiveness of internal controls, about the quality of evidence, and so on. These uncertainties or risks are commonly classified as inherent risks, control risks, or detection risks.

Assessing the degree of risk present and identifying the areas of highest risk are critical initial steps in detecting financial statement fraud. The auditor specifically evaluates fraud risk factors when assessing the degree of risk and as noted in previous chapters, approaches this risk assessment with a high level of professional skepticism, setting aside any prior beliefs about management's integrity. Knowing the circumstances that can increase the likelihood of fraud, as well as other risk factors, should aid in this assessment.

Fraud Risk Factors

SAS 99 identifies fraud risk categories that auditors may evaluate in assessing the risk of fraud. The three main categories of fraud risk factors related to fraudulent financial reporting are management characteristics, industry characteristics, and operating characteristics, including financial stability.

1. *Management characteristics* pertain to management's abilities, pressures, style, and attitude as they have to do with internal control and the financial reporting process. These characteristics include management's motivation to engage in fraudulent financial reporting—for example, compensation contingent on achieving aggressive financial targets; excessive involvement of nonfinancial management in the selection of accounting principles or estimates; high turnover of senior management, counsel, or board members; strained relationship between management and external auditors; and any known history of securities violations.
2. *Industry characteristics* pertain to the economic and regulatory environment in which the entity operates, ranging from stable features of that environment to changing features such as new accounting or regulatory requirements, increased competition, market saturation, or adoption by the company of more aggressive accounting policies to keep pace with the industry.
3. *Operating characteristics and financial stability* encompass items such as the nature and complexity of the entity and its transactions, the geographic areas in which it operates, the number of locations where transactions are recorded and disbursements made, the entity's financial condition, and its profitability. Again, the auditor would look for potential risk factors such as significant pressure on the company to obtain additional capital, threats of bankruptcy, or hostile takeover.

The two primary categories of fraud risk factors related to asset misappropriation are susceptibility of assets to misappropriation and adequacy of controls.

1. *Susceptibility of assets to misappropriation* refers to the nature or type of an entity's assets and the degree to which they are subject to theft or a fraudulent scheme. A company with inventories or fixed assets that include items of small size, high value, or high demand is often more susceptible, as is a company with easily convertible assets such as diamonds, computer chips, or large amounts of cash receipts or cash on hand. Cash misappropriation is also included in this category through fraudulent schemes such as vendor fraud. (See Chapter 17.)

2. *Adequacy of controls* refers to the ability of controls to prevent or detect misappropriations of assets, owing to the design, implementation, and monitoring of such controls.

SAS 99 discusses fraud risk factors in the context of the *fraud triangle*, a concept first discussed in Chapter 2. Additionally, SAS 99, paragraph 40, suggests considering the following attributes of risk:

- Type of risk that may be present—that is, fraudulent financial reporting, asset misappropriation, or corruption
- Significance of the risk—that is, whether it could result in a material misstatement
- Likelihood of the risk
- Pervasiveness of the risk—that is, whether it relates to the financial statements as a whole or to particular accounts, transactions, or assertions

Management's selection and application of accounting principles are also important factors to consider.

A Word on Information Technology

The effective use of information systems and technology pervades all five COSO framework components (discussed in Chapter 6) and is integral to an effective antifraud program. From an information technology (IT) perspective, the more complex a company's system environment is, the more susceptible the organization may be to fraud. With regard to determining the "ability to commit fraud," IT security controls are examined with particular emphasis on the way security is administered in an organization. Security systems are one way that organizations accomplish segregation of duties, a cornerstone of good internal controls. Historically, most large and complex organizations are not good at this. Poor administration controls—over who should or should not have access to data—inevitably lead to inappropriate access. Once that happens, the vehicle to commit the fraud comes into being, providing the opportunity for other motivational factors to kick in. (See discussion of the fraud triangle, Chapter 2.) Moreover, if other problems exist within IT—for example, problems in change control and ease of system access—disguising fraud could be relatively easy.

INTERPRETING POTENTIAL RED FLAGS

Of course the interpretation of red flags is not easy. It may sound easy, but in the real world of business it is very difficult. First, the word *flags* is a bit of a misnomer and creates a false impression of plainly visible warning signs. While this is true of some frauds, it is important to remember that fraud is fundamentally a crime of deception and deceit. Calling to mind a mental picture of a scarcely visible red thread waving in the wind is more accurate than picturing a bold red flag. Some of the difficulties

inherent in identifying and interpreting potential red flags are summarized in the following:

- *Fraud risk factors are not the same as evidence of fraud.* Risk factors are not evidence of fraud. To the extent that risk factors are evidence of anything, they point to an environment or situation in which there is an increased risk that material misstatement due to fraud might occur either generally or in a specific functional or geographic sector of the entity's operations.

  Individuals may be motivated by the prospect of bonuses and other incentives to manipulate results to their advantage and in a manner that may amount to fraud. Several high-profile instances of financial statement fraud have been motivated in part by bonus and incentive arrangements. As an example, a chairman and CEO was accused of earning substantial bonuses and profiting on the sale of shares in the company on the basis of fraudulent financial reporting that misrepresented the company's results. This does not mean, of course, that the presence of bonus and other incentive schemes is prima facie evidence of fraudulent financial reporting, but it may be considered in the overall risk assessment.

  Another example of a fraud risk factor is the so-called dominant CEO. Over the years—in a number of notorious cases, including the collapse of the Robert Maxwell empire—a larger-than-life individual apparently held sway over a cowed and ineffectual board and senior management, which enabled him to perpetrate or preside unchecked over a material financial reporting fraud. Even absent a dominant CEO, similar risks can emerge whenever corporate governance is weak—for example, when power is concentrated in the hands of senior management without an effective counterbalance from the board. No one would seriously suggest, however, that the existence of a CEO with a forceful personality and a strong sense of mission is indicative of fraud. It is simply a risk factor.
- *Fraud risk factors may indicate the existence of risks other than fraud.* Many risk factors are not exclusively indicative of fraud risk. They may also suggest a heightened risk of material misstatements due to human or process error. For example, deficiencies in internal controls may be regarded as fraud risk factors, but they also pose the risk that errors may occur and go undetected without any intent to commit fraud. Sometimes weak internal controls simply fail to limit or identify accounting or reporting mistakes. The auditor should not discount either possibility without reasonable grounds for doing so.
- *Fraud risk factors can be ambiguous.* Many fraud risk factors are susceptible to both innocent and sinister interpretations. The fact that a company has a complex structure with a large number of overseas subsidiaries and significant intracompany trading may indicate an increased fraud risk, or it may simply be a legitimate characteristic of that business. On one hand, that a ledger clerk drives a car he appears to be unable to afford may indicate a risk that he has misappropriated company assets. On the other hand, he and his wife may have a two-income household that allows them certain luxuries. The focus must be on fact-finding and critical assessment of cumulative evidence, not unfounded speculation driven by the existence of risk factors.

- *There is no linear relationship between the number of fraud risk factors and the level of fraud risk.* It may be that, in general, the more risk factors the auditor identifies in a client, the greater the overall risk of fraud. But even a few risk factors in key areas may be grounds for concern. A simplistic attempt to quantify fraud risk by a count of risk factors is misguided. The objective is not to estimate how likely it is that a material misstatement due to fraud will occur but, rather, to identify where and in what manner that might happen.
- *Fraud risk factors are of limited significance in isolation.* In general, individual risk factors are of limited significance in isolation. Rather, they need to be considered as a whole. The point about the dominant CEO factor, for example, is that it may actually contain a number of separate risk factors that when looked at together, create a risk situation: a bullying CEO, lack of counterweight among other senior executives, and apparent absence of an effective audit committee, supervisory board, or similar corporate governance function. The auditor attempts to interpret evidence of potential risk factors within the wider context of other observations about the company, its management, and the business environment in which it operates. Nonetheless, the identification of an anomaly or loose thread can lead to the identification of multiple risk factors and control weaknesses or actual instances of financial statement fraud or misappropriation of assets. The auditor considers whether one particular risk factor may, in fact, be linked to one or more other factors.
- *Some fraud risk factors are very difficult to observe.* Certain fraud risk factors are essentially states of mind or related to an individual's private life or personal financial affairs. They may be impossible to observe directly. The auditor might nonetheless become aware of indirect signs that relevant states of mind or private-life factors may exist.

All of these issues increase the challenge faced by the auditor in trying to identify indications of the existence of fraud risk within the substantial body of information available from the audit process.

SAS 99 distinguishes between risk factors relevant to the risk of material misstatement due to fraudulent financial reporting and those relevant to the risk of material misstatement arising out of the misappropriation of assets. In practice, as the standard acknowledges, many risk factors are potentially common to both kinds of misstatement. Risk factors related to weaknesses in control or supervision may, for example, be equally applicable to either type of fraud.

IMPORTANCE OF PROFESSIONAL SKEPTICISM

According to SAS 1, *Codification of Auditing Standards and Procedures,* adequate professional care means that the auditor exercises professional skepticism. This attitude has always been a cornerstone of auditing standards, and the current environment, characterized by increased complexities and risks, creates a heightened sense of its importance. As discussed in Chapter 11, professional skepticism is a key attribute of an effective auditor. SAS 99 and other standards emphasize the importance of professional skepticism in the consideration of fraud risk. SAS 99 offers examples of skepticism at work: "Thoroughly probe the issues, acquire additional evidence as

necessary, and consult with other team members and, if appropriate, experts in the firm, rather than rationalize or dismiss information or other conditions that indicate a material misstatement due to fraud may have occurred."[7]

By definition, fraud involves the use of deception. This may take the form of manipulated or falsified accounting records and vouchers, improper accounting or disclosure, or false, inaccurate, or incomplete explanations. While auditors are not required to assume that they are being lied to or that documents provided to them are false[8]—absent indications that such may be the case—they challenge explanation or documentary evidence that is inconsistent with information from other credible sources inside or outside the client organization or with their well-founded expectations based on prior experience or knowledge. When such inconsistencies arise, SAS 99 is explicit[9]—and experience suggests that auditors will not simply accept the evidence offered because they believe the individual concerned, or management generally, to be honest.

Professional skepticism has several aspects: keeping an open mind, developing a heightened awareness, making a critical assessment of evidence, and seeking corroboration.

Auditors keep an open mind and avoid preconceived notions about the entity or its management.[10] This approach in no way undermines the importance of cumulative audit knowledge in relation to a client or familiarity with the people responsible for management; both are important elements in the identification and evaluation of risk factors. How an entity has operated and how management has behaved in previous periods may be good indicators of what the auditor may expect in the period currently subject to audit.

Or they may not be. Circumstances change, and so does the way people behave. The auditor is alert to this possibility and is able to identify warning signs as they arise. While the auditor is not required to assume that management is dishonest—in the absence of any evidence to that effect—such a possibility may not be altogether discounted; neither should positive indicators of dishonesty—or the risk thereof—be ignored because of a prior belief that So-and-So would not commit fraud. Naturally, the converse also applies. The auditor should not rush to judgment in situations in which risk factors are identified. Further analysis, fact-finding, and testing often lead to the conclusion that despite the presence of certain risk factors, no material misstatement resulting from fraud has arisen.

Developing a heightened awareness of fraud risk helps the auditor maintain professional skepticism. Knowing the kinds of things that can go wrong—based on, among other things, analysis of the corporate scandals of the last decade—and

---

[7] Id., par. 16.

[8] Id., par. 9, "An audit conducted in accordance with GAAS rarely involves the authentication of such documentation, nor are auditors trained as or expected to be experts in such authentication."

[9] Id., par. 13.

[10] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, par. 13, states: "The auditor should conduct the engagement with a mind-set that recognizes the possibility that a material misstatement due to fraud could be present, *regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity*." [emphasis added]

relating that knowledge to a specific client can be an important tool in detecting fraud.

The auditor should critically assess the evidence gathered at all stages of the audit by using professional judgment to determine whether sufficient appropriate audit evidence has been obtained upon which to draw conclusions. In addressing an area in which factors indicating a risk of material misstatement due to fraud have been identified, the auditor carefully considers whether circumstances demand a greater quantity or quality of audit evidence to obtain a reasonable level of assurance as to the completeness or accuracy of a particular balance, transaction, or other item. To do this, the auditor assesses all of the available evidence and considers whether, taken together, it provides the appropriate level of assurance.

It is important to corroborate management's explanations with evidence from other credible sources, including third parties, when appropriate and possible. This is consistent with existing auditing standards, which recognize that third-party evidence is generally more reliable than evidence created by the entity itself.

The auditor's attitude is one of professional skepticism. It is worth recalling here several key formulations in SAS 99: "The auditor should conduct the engagement with a mind-set that recognizes the possibility that a material misstatement due to fraud could be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity."[11] This is particularly important in light of the situation that "management has a unique ability to perpetrate fraud because it is frequently in a position to directly or indirectly manipulate accounting records. . . . Fraudulent financial reporting often involves management's override of controls that otherwise may appear to be operating effectively. Management can either direct employees to perpetrate fraud or solicit their help in carrying it out."[12] SAS 99 specifically calls for an auditor mind-set of neutrality in conducting audit procedures, recognizing that the perceived character of the client should never be a substitute for obtaining objective evidence.

Probing and explicit questions about fraud risks and the possibility of fraud are contemplated by SAS 99. They may be asked during interviews with management and key financial staff. For example, to probe the fraud risk factor of pressure to meet budget,[13] such questions might include the following:

Sample Questions for Management

- How were goals or budgets or both achieved during a down economy?
- What did your company do differently from its competitors to obtain revenue or earnings-per-share goals when the rest of the industry was not meeting expectations?

---

[11] Id.

[12] Id., par. 8.

[13] Comparing budget with actual is an important analytic procedure discussed later in this chapter. From a fraud perspective, such a comparison is important for several reasons. A common fraudulent financial statement scheme involves falsification of revenues to meet budget. A common asset misappropriation scheme involves stealing up to a budgeted amount. In both cases, just because a reported amount for a budgeted line item appears to be in line with the expected amounts for that line item does not ensure the absence of fraudulent activity.

- Were any changes implemented during the quarter so that goals or budgets or both could be achieved? For example, were new customers obtained or were cost-cutting measures implemented?
- What specifically caused the company to meet goals or budgets or both?

Sample Questions for Financial Staff

- Do you ever feel pressured to maintain the books and records with an eye toward managing actual expenses or revenues to be in line with budgeted expenses or revenues?
- Can you give an example of instructions from management that may have made you feel uncomfortable?[14]

It is also generally advisable to probe management and other financial staff regarding the overall ethical environment of the organization. Does a written code of ethics exist? Are top managers and employees required to periodically confirm that they are in compliance with the code of ethics? Do top managers and employees receive training in the code of ethics? Have disciplinary actions been taken related to violations of the code? All of these are legitimate and pertinent questions.

A mind-set of professional skepticism may result in taking additional steps while performing analytic procedures and detail testing to corroborate management's assertions. Analytic procedures discussed later in this chapter identify testing or analysis that could assist the auditor in evaluating the reasonableness of management's assertions and could provide corroborating or contradictory information. Additional corroboration could come from interviews of personnel from different departments, including nonaccounting personnel. Critically assessing all evidence and seeking verifications of assertions are standard procedures in the effort to detect a fraudulent transaction.

REVISITING THE FRAUD TRIANGLE

In the context of this discussion of potential red flags, it is worthwhile to revisit the concept of the fraud triangle. As you will recall, SAS 99 identifies three categories of risk—the fraud triangle—and views them as key conditions that tend to be present when fraud occurs.[15]

---

[14] Recognize that a question of this type is provocative and anticipates that something inappropriate may have occurred. Interviewing techniques are discussed briefly later in this chapter but are addressed in detail in Chapter 18 of this book. Such provocative questions may not be used in all circumstances.

[15] ISA 240 (see footnote 4) identifies a broadly similar range of risk factors but categorizes them differently. Risk factors concerning the risk of material misstatements resulting from fraudulent financial reporting are arranged under the headings "Management's Characteristics and Influence over the Control Environment," "Industry Conditions," and "Operating Characteristics and Financial Stability." Risk factors concerning the risk of material misstatements resulting from misappropriation of assets are grouped under "Susceptibility of Assets

1. Incentive and pressure, that is, need
2. Opportunity
3. Rationalization and attitude

Within each of these broad risk categories, many different and specific potential red flags may be visible within a company.

Incentive and Pressure

Management or other employees may find themselves offered incentives or placed under pressure to commit fraud. When, for example, remuneration or advancement is significantly affected by individual, divisional, or company performance, individuals may have an incentive to manipulate results or to put pressure on others to do so. Pressure may also come from the unrealistic expectations of investors, banks, or other sources of finance.

Certain risk factors are usefully considered in the evaluation of whether or not the organization is at a greater or lesser degree of risk, owing to incentives or pressures that could potentially lead to material misstatements. These risk factors include:

- Circumstances that threaten the profitability or financial stability of the business
- Excessive pressure on management to meet or exceed the expectations of third parties, including investors and lenders
- Significant threats to the personal wealth of management as a result of the performance of the business
- Excessive internal pressures on divisional or departmental management imposed by the board of directors or senior management
- A struggle to retain the company's listing on a stock exchange or debt rating
- Inability to meet debt covenants or satisfy conditions in merger or acquisition agreements

Incentive and pressure can take a variety of forms within an organization: bonuses or incentive pay representing a large portion of an employee's or group's compensation; triggers built into debt covenants tied to share price targets and levels; significant stock option awards throughout the organization but particularly to top management; and aggressive earnings-per-share and revenue targets set by top management and communicated to analysts, investment bankers, and other market participants, with resultant pressure from these groups.

With regard to the risk of material misstatement due to misappropriation of assets, the risk factors are:

- Personal financial problems that might motivate an individual to misappropriate assets
- Adverse relationships between the entity and one or more of its employees, which might create feelings of resentment or disloyalty

---

to Misappropriation" and "Controls." These headings were used in the old SAS 82 [ISA 240, Appendix 1].

Personal pressures have increased significantly in recent decades as stock options became a common means of compensating and motivating management. Many managers today have a large portion of their compensation and even their net worth tied to the performance of the company and, specifically, the performance of the company's stock. As a result of compensation and retirement contributions in the form of stock grants and as a result of stock ownership and personal debt secured by stock, the financial position of many managers is inextricably tied to the financial performance of their employer.[16] Fear of losing one's position or of delivering bad news, the desire to be promoted, personal financial obligations, or simply greed[17] can also be the driving forces behind fraudulent activity.

Determining the presence and degree of these pressures or incentives is part of the auditor's goal in evaluating the risk that misstatements due to fraud may have occurred. Keep in mind that some people will go to extraordinary lengths to satisfy their needs. The ability to satisfy those needs through inappropriate measures is increased if the other components of the fraud triangle are present.

Opportunity

Circumstances may exist that create opportunities for management or other staff to commit fraud. When such opportunities arise, those who might not otherwise be inclined to behave dishonestly may be tempted to do so. Even individuals under pressure and susceptible to incentives to perpetrate a fraud are not a grave threat to an organization unless an opportunity exists for them to act on their need. An opportunity must exist to commit fraud, and the fraudster must believe the fraud can be committed with impunity. Absent or ineffective controls, lack of supervision, or inadequate segregation of duties may provide such opportunities. Opportunities may also be inherent in the nature, size, or structure of the business. Certain types of transactions lend themselves more than others to falsification or manipulation, as do certain kinds of balances or accounts. Certain corporate and group structures may be more opaque and susceptible to misuse. And certain types of asset are more prone to misappropriation.

Risk factors indicative of opportunities that could lead to material misstatements as a result of fraudulent financial reporting include:

- Factors related to the nature of the industry in which the entity operates, the nature of the entity's business and the transactions it enters into, and the manner in which they are recorded in the profit-and-loss account or balance sheet.
- The nature of the entity's relationships with customers and suppliers and its position in its markets: The ability to dominate or dictate terms may create the opportunity for inappropriate or other transactions not at arm's length.

---

[16] In one example, key officers of a publicly traded company were pressured to make significant purchases of company stock to signal to Wall Street their confidence in the company's prospects. These stock purchases were financed with loans collateralized by the stock. The loans were callable if stock prices fell below a certain point. This was strong incentive to maintain the stock prices.

[17] Some people, regardless of their income level, live beyond their means. Maintaining their standard of living becomes a need they may seek to fulfill regardless of methods.

- The degree of judgment involved in determining the level of income or expenditure or the valuation of assets or liabilities: Generally, a higher degree of judgment will give rise to a greater opportunity for deliberate manipulation.
- The extent and effectiveness of supervision of senior management by independent corporate governance functions such as the audit committee, nonexecutive directors, and supervisory boards.
- The degree of complexity and stability of the entity or group.
- The overall control environment, including the continuity and effectiveness of internal audit, information technology, and accounting personnel as well as the effectiveness of accounting and reporting systems.

In several large financial statement fraud cases, opportunity existed by virtue of management's role in the internal control structure and its ability to override or avoid existing controls. With regard to the risk of material misstatement resulting from misappropriation of assets, the risk factors best categorized as related to opportunity can be summarized as follows:

- Susceptibility of fixed assets, inventories, or other assets to misappropriation, depending on such variables as value, demand, portability, and convertibility
- Weaknesses in the controls designed to safeguard assets, such as supervision, segregation of duties, employee screening, physical controls, reconciliations, and other accounting controls

Rationalization and Attitude

Some individuals are more prone than others to commit fraud. Other things being equal, the propensity to commit fraud depends on a person's ethical values as well as on their personal circumstances. Ethical behavior is motivated both by a person's character and by external factors. External factors may include job insecurity, such as during a downsizing, or a work environment that inspires resentment, such as being passed over for promotion. The external environment also includes the tone at the top—the attitude of management toward fraud risk and management's responses to actual instances of fraud. When fraud has occurred in the past and management has not responded appropriately, others may conclude that the issue is not taken seriously and they can get away with it.

Risk factors that fall into this category of rationalization and attitude are typically the least tangible or measurable, and many are by nature difficult for an auditor to observe or otherwise ascertain. Fundamentally, rationalization and attitude are functions of the culture of an organization, the psychology of those who work in it, and the interaction between the two—for example, the level of employee loyalty to the company. The wider business environment must also be considered: Hard times in an industry or in the overall economy may make it easier for some individuals to rationalize fraud. Risk factors to look for, in this somewhat intangible but critically important category, include:

- Lack of clarity or communication about corporate ethical values or infrequent communication and reinforcement of such values
- Disregard for the risk of fraud—or ineffective measures when fraud rises

- Lack of realism in budgeting and forecasting and in communicating expectations to third parties
- Recurring attempts by management to justify inappropriate accounting or disclosure policies and practices on grounds of materiality or other grounds
- Difficult relationships with the entity's auditors: a bullying attitude, imposition of unreasonable time pressure, or constraints on access to relevant audit evidence

Most frauds begin small and build over time. Many people can easily rationalize small infractions such as using the office phone for personal long-distance phone calls or stocking their home office with supplies from the company supply cabinet—and the auditor will come into contact with individuals who are, of course, capable of these rationalizations. These rationalizations can be simple, even for a complex financial crime. Some of the most common rationalizations prove to be the following:

- It is just temporary.
  - The company will do better next quarter and the act can be reversed. No one will ever know.
  - It is not really fraud, right, if I book this entry one month and then reverse it the next? In the end, it washes and no one's harmed. The company stays in compliance with debt covenants, and we make our dividend payments.
- Management does not care.
  - Management does not seriously monitor internal controls.
  - Management does not correct known deficiencies in controls.
  - Management does not discipline this kind of behavior.
- Management participates in, expects, and rewards this kind of behavior.
  - Management has entered into certain transactions purely for the purpose of meeting specific reporting objectives.
  - Management traditionally uses aggressive accounting policies, and we need to remain consistent with prior periods.
  - The people being promoted helped the company achieve its objectives without regard to the means of getting there.
  - Risk taking is rewarded. We are cowboys—but nobody is allowed to say that anymore.
- No one is hurt and the company is helped.
  - It is not material to the company as a whole. But it makes a huge difference to our proceeds from the public offering.
- I deserve this.
  - I was passed over for the promotion I deserved.
  - I'm paid at less than the market rate for my services and the value I provide.
  - The company has no loyalty to its employees; I'm likely to be laid off soon.
  - This will make up for the benefits the company just eliminated.

Determining whether a basis exists to rationalize a fraudulent act is a key part of the evaluation of the risk that misstatements due to fraud may have occurred.

Typically, all three conditions of the fraud triangle will be present in varying degrees when fraud occurs. They are closely related. When the incentive to commit fraud is strong, it is likely to be easier for perpetrators to rationalize their actions. Easy opportunity may have a similar effect: When internal controls are absent or

ineffective, an employee may conclude that management is indifferent to fraud—that nobody cares. The greater the extent to which all three conditions are present, the greater the likelihood that fraud will occur. Cultivating an environment that minimizes these conditions is vital to avoiding or limiting fraud risk. Even if one or more conditions are absent, however, fraud risk is not eliminated. The incentive or pressure may be such as to drive an individual or group to commit fraud despite the absence of easy opportunities to do so. Similarly, predators (see Chapter 2) may not need to rationalize their depredations on a firm; it just comes naturally.

IDENTIFYING AND EVALUATING RISK FACTORS

As noted earlier, fraud risk factors need to be evaluated in context. That context can be defined as an understanding of the business of the entity and the general economic and market environment in which it operates; the presence of other fraud risk factors, if any; and the existence and effectiveness of mitigating controls. Facts or circumstances that may constitute fraud risk factors in one context may have less significance in another. For example, a small owner-managed entity is likely to have in place less-sophisticated corporate governance structures and systems of internal control than is a large multinational organization. Basic elements such as independent supervision of management—such as by way of an effective audit committee—and segregation of duties between key operational and accounting functions may not be as well developed and may not even be practical in a smaller entity. Such matters might be cause for concern in a larger organization, but in a smaller one, their potential impact on fraud risk may be at least partially offset by the closer involvement of the owner-manager and perhaps by cultural differences.

An adequate understanding of the entity's business and its relationship with business partners, suppliers, and customers is crucial to the proper evaluation of fraud risk factors. The ability to identify unusual or suspicious transactions, questionable financial ratios, and implausible explanations by management or others clearly implies an awareness and understanding of what is normal and expected in the context of the entity, the industry sector, and the general business and economic environment in which the entity operates.

The auditor also considers the accumulation of fraud risk factors. For example, that a significant portion of management's remuneration is in the form of bonuses or stock options linked to so-called aggressive targets of one kind or another is listed as a fraud risk factor in SAS 99. Yet such arrangements are common in publicly listed companies and often viewed as effective ways of aligning the interests of management with those of stockholders. Furthermore, the aggressiveness of targets may not be easy to judge. Therefore, in isolation, this risk factor may not immediately set alarm bells ringing. But if the auditor were to conclude that the audit committee was insufficiently robust in its stance vis-à-vis management decisions, and that management—including nonfinancial management—appeared to be exerting undue influence over accounting policies in a manner likely to distort key financial measures in their favor, then the cumulative effect of these circumstances might be more persuasive of the existence of a risk of material misstatement due to fraud.

In the immediately preceding example, the observed fraud risk factors exemplify the first two conditions of the fraud triangle: incentive and opportunity. While the

presence of all three conditions is not a prerequisite to the existence of a significant risk of material misstatement due to fraud, the example illustrates that the presence of even two conditions tends to create more persuasive grounds for concern.

The evaluation of the impact of fraud risk factors on the level of audit risk also involves consideration of any internal controls that might mitigate the risk of material misstatement due to fraud. Knowledge of controls will be drawn both from the auditor's cumulative audit knowledge and experience and from the results of the examination and testing of controls during the current audit. The additional internal control focus required by Sarbanes-Oxley will provide a further source of information on the internal control environment and may highlight gaps in the internal control structure that need to be considered from a fraud risk perspective.

In placing reliance on a control to mitigate the risk of fraud, auditors may satisfy themselves that the control would, if operated properly, mitigate the risk in question and that the control has operated effectively during the period subject to audit. Even if auditors can obtain reasonable assurance on these counts, they should not discount the possibility that management or others may override controls or otherwise circumvent normal processes to manipulate results or balances.

The identification and evaluation of fraud risk factors should not be seen as a one-time-only process carried out and completed at the planning stage. Rather, it is a cumulative process that continues through the audit. Auditors remain alert to the risk of material misstatement resulting from fraud at all stages of the audit so that their assessment may be updated in the light of new information. Such information may emerge:

- During planning and risk assessment
- In discussions with management or other employees
- As a result of controls testing or substantive analytic or detailed testing at the review or audit completion stage

The audit engagement leader ensures that a mechanism is in place within the audit team for the sharing of information concerning potential fraud risk factors—or evidence of fraud—so that any such information is brought forward and can be considered in a broader context. This helps ensure that the existing assessment of fraud risk is reevaluated regularly in light of new evidence. To achieve these goals, the audit team holds discussions about the risk of material misstatement due to fraud and the need to apply healthy professional skepticism at all times. As noted earlier, this step is actually set out under SAS 99. On larger audit assignments, in particular those whose audit team is divided among different locations or operating units, it may be advisable to establish procedures for channeling information about potential fraud risk factors, so that the information is readily available to the audit engagement leader and those assisting in the management of the audit. The team might also establish a formal step during audit completion to discuss the cumulative evidence.

Discussion among Audit Team Members

Because discussion within the audit team is a required part of the audit process, it bears a closer look. SAS 99 instructs that such a discussion take place and include

an exchange of ideas about how the entity's financial statements "might be susceptible to material misstatement due to fraud, how management could perpetrate and conceal fraudulent financial reporting, and how assets of the entity could be misappropriated."[18] SAS 99 also calls on the audit team to emphasize how to maintain "the proper state of mind throughout the audit regarding the potential for material misstatement due to fraud."

The discussion of the entity's susceptibility to material misstatement due to fraud is expected to encompass consideration of fraud risk factors discussed in this chapter and SAS 99. It is also intended to cover the risk that management might override controls and set aside any previously held views concerning management's integrity. The discussion should also address how the audit team proposes to respond—such as with additional or alternative procedures—to any fraud risk factors identified at this stage.

While SAS 99 does not prescribe the manner in which the importance of professional skepticism is to be conveyed to the audit team in the course of the discussion, a reasonable approach might involve touching on each of the following issues, perhaps with the help of illustrative examples:

- Impact of any issues emerging from the client acceptance or client continuance assessment.
- Past experience: any frauds or accounting errors uncovered previously.
- Assessment of the quality of accounting and reporting personnel or client employees involved in the internal control structure.
- Fraud risk factors set out in the relevant guidance: Attendees might consider these factors in advance to allow for informed discussion during the meeting.
- The information needed for assessing the risk of material misstatement due to fraud and how it will be gathered. Options include:
  - Inquiries of management
  - Analytic procedures
  - Consideration of any fraud risk factors identified
  - Other sources
- Additional steps required:
  - Using information obtained to identify fraud risk
  - Assessing fraud risks identified, taking into account an evaluation of relevant controls, including the risk of management override of controls
  - Responding to the results of the assessment through additional procedures or other responses, as appropriate
  - Evaluating audit evidence
- Indicators to look out for, and what to do about them.
- The audit engagement leader's reaffirmation of the importance of professional skepticism at all stages of the audit.
- How to document audit work in relation to the consideration of fraud risk.
- Points to take from the team meeting and incorporate into the audit-planning process.

[18] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, pars. 14–18.

Not all of these points will be relevant in every case. The auditor has discretion to decide whether to deal with the points in one or more separate meetings or as part of a larger meeting.

INFORMATION GATHERING

SAS 99 suggests that the key sources for the identification of fraud risk factors are inquiries of management and others, analytic procedures, consideration of fraud risks, and other information available within or about a specific company.[19] The expression *management and others* encompasses executive management, the audit committee, and internal audit, as well as others within the organization who might be expected to have relevant views, including those involved in operational matters rather than directly involved in the financial reporting process.

SAS 99 has the effect of amending the requirements of SAS 85 concerning the nature of representations that the auditor obtains from executive management.[20] Among the questions the auditor might well raise with management, the following would be among the most important:

- Does management have knowledge of any fraud—whether related to financial reporting or to asset misappropriation—perpetrated, alleged, or suspected that could result in a material misstatement of the entity's financial statements?
- Regardless of materiality, does management have knowledge of any fraud perpetrated, alleged, or suspected?
- Has management received any letters or communications from employees, former employees, analysts, short sellers, or others concerning allegations of fraud?
- What is management's understanding of the risks of fraud in the company?
- Are there any specific fraud risks the company has identified or any account balances or classes of transactions for which a risk of fraud may be more likely to exist, and why?
- What programs and controls has management established to mitigate specific fraud risks that have been identified or to help prevent, deter, and detect fraud of other kinds? How does management monitor those programs or controls?
- How does management communicate its views on business practices and ethical behavior?
- How does management demonstrate behavior consistent with its views?
- What procedures are in place to monitor the operating locations or business segments of the business? Are there any particular subsidiary locations or business segments in which the risk of fraud is more likely?
- Has management reported to the audit committee—or to others with equivalent authority and responsibility for the entity's internal control—concerns about how management believes the internal control framework serves to prevent, deter, or detect material misstatements due to fraud? The report would be likely

[19] Id., pars. 19–34.
[20] Id., Appendix, Amendment to SAS 85, *Management Representations* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 333), par. 6, and Appendix A.

to include the entity's control environment, risk assessment process, control activities, information and communication systems, and monitoring activities.
- Has anyone asked a member of management or others within the company to withhold information from the auditor, alter documents, or make fictitious entries in the books?

When appropriate, the auditor should ask management either to provide corroborative evidence for its answers to these questions or to indicate where and how such evidence might be obtained. When answers are given in general terms, the auditor may ask for specific examples. The auditor should also be alert to answers that appear evasive or otherwise indicate that management does not take the risk of material misstatement due to fraud as seriously as might be expected. These signs do not necessarily indicate a lack of honesty or integrity on the part of the respondent—or they may indicate precisely that. At the very least, they may raise the concern that management underestimates the risk and, as a consequence, the auditor may find that important areas of corporate governance or control are less than wholly effective.

Inquiries of management and others in the context of identifying potential fraud risk factors are not interviews conducted in the style of a forensic accounting investigator (see Chapter 8). However, application of some of the same basic principles may not be out of place. In particular, the auditor may ask a combination of open and closed questions, the former to elicit a broad answer and the latter to focus on particular aspects or to confirm or clarify specific matters. The auditor listens carefully to answers and responds to them with follow-up questions. A checklist approach to such discussions is unlikely to be as useful or effective as this more searching, iterative approach.

The auditor should keep in mind that the views of management concerning fraud risk may vary with the level of management. For example, divisional management, responsible for divisional results that contribute to the overall profit-and-loss account and balance sheet, may provide the auditor with a different perspective from that of senior management. Divisional management may be subject to different incentives or pressures and may have a different attitude toward fraud risk yet may be a valuable source of information in the context of a review of adjusted journal entries at the corporate level whether by providing satisfactory explanations of what it is that particular adjustments represent or by an inability to provide such explanations.

To the audit committee, the auditor might pose these questions:

- What are the audit committee's views regarding the risk of fraud?
- Is the audit committee aware of any fraud perpetrated, alleged, or suspected?
- How does the audit committee exercise oversight over activities concerned with the risks of fraud and the programs and controls established to mitigate risks?
- What is the audit committee's assessment of management's performance in this regard?

As with management, the auditor may seek to corroborate answers, when appropriate, and bear in mind that the answers are likely to provide not just information but also an indication of the audit committee's awareness and effectiveness. In the

aftermath of almost a decade of corporate scandals, the composition and responsiveness of audit committees have changed. Audit committees are becoming increasingly sensitized to issues of financial misstatement and impropriety, although there are always exceptions. The auditor should be mindful of situations in which the audit committee attempts to steer the auditor to accept a certain outcome.

A similar approach can be taken with the organization's internal audit function. Internal audit personnel were key in identifying financial statement errors at WorldCom. However, a company with a large staff of internal auditors may not be particularly skilled in risk assessment or in conducting an investigation into financial accounting irregularities or other fraud. Some internal auditors use sophisticated tools and techniques and adopt an active approach to risk assessment. Others, including those at many major companies, may be considerably less sophisticated.

It is important to gain a comprehensive understanding of where the internal auditors spend their time. In the case of multinational entities, the external auditor may gain an understanding of what internal audit is doing in each location. Questions designed both to bring to light specific instances of fraud and to assist the auditor in assessing the effectiveness and independence of internal audit might include:

- What are internal audit's views regarding the risk of fraud?
- What specific internal audit procedures have been performed to prevent, deter, or detect fraud?
- What were the results of this work?
- Is internal audit aware of any instances of fraud perpetrated, alleged, or suspected?
- Has management responded satisfactorily to internal audit findings throughout the year?
- Have there been any limitations with respect to what internal audit can review or when the review can take place?

Questions to be asked of others within the organization will be tailored to their areas of knowledge and their positions in the company. While people lower in the hierarchy may not have the same overview as senior management, their views should not be disregarded or discounted. They may have a more detailed understanding about the operation of particular controls, perhaps because they're directly involved with them. In instances in which management is the perpetrator of the fraud, lower-level personnel may know what is going on or can direct the audit team to relevant documents or transactions.

The auditor may consider the possibility that the company's general counsel may have relevant information or views. If frauds or other reportable events have occurred in the past, it is likely that in-house counsel will be aware of this. Indeed, they're likely to have been involved in any remedial or other steps taken. In-house counsel may also be aware of any regulatory or other proceedings involving the entity that may have a bearing on the financial statements. Legal counsel, a compliance officer, or human resources may have details of investigations and ethics violations. And there may be instances of suspected embezzlement that were handled through these channels. Others in management, especially new management, may not be aware of such ethics violations.

Other Sources

In specific cases, other potentially relevant sources of information or procedures may also be available to the auditor, such as:

- General press and media reports that indicate the existence of concerns about matters directly or indirectly related to the entity's financial statements.
- Specialist industry publications and trade journals.
- Analysts' reports.
- Legal and litigation data.
- Data mining (see Chapter 17), which may be useful in identifying transactions for further review, especially when fraud risk may be high: Data mining can identify high-dollar round numbers that could be journal entries booked at the end of a period. In selecting such journal entries for testing, the auditor may encounter a lack of support or an explanation revealing between the lines that the purpose of the entries was to make the numbers for the period.
- Public records searches and background checks (see Chapter 15) for verifying the existence of a customer, supplier, or employee: They may identify undisclosed conflicts of interest, ownership of real estate, judgments, liens, and more. (Many free and fee-based databases contain public records and information, but searching them and interpreting the results can be an art. The skilled professional knows which databases to access in a cost-efficient and cost-effective manner.)

The extent to which the auditor incorporates such sources into the audit approach will be a matter of professional judgment, taking into account what is practical and reasonable in the circumstances.

Information gathering and identification of fraud risk factors may be inseparable processes in practice. On one hand, the auditor may already have a view as to those areas of the entity's financial statements that are subject to greater-than-average risk of material misstatement due to fraud, and this view may lead the auditor to seek specific information and analysis or to intensify information-gathering efforts in a particular area. On the other hand, the information obtained may lead to the identification of fraud risk factors not previously identified. Given the iterative nature of the process, the distinction between the information-gathering phase and the identification of fraud risk factors becomes somewhat artificial. The auditor's objective, by all available means, is to identify any fraud risk factors within the body of information available, much of which the auditor will probably gather for other audit-related purposes.

ANALYTIC PROCEDURES

Analytic procedures represent one of the most important detection techniques.[21] SAS 56 (AU Section 329.02) defines these procedures as "evaluations of financial information made by a study of plausible relationships among both financial and nonfinancial data. . . . A basic premise underlying the application of analytic procedures

[21] In addition to the discussion that follows, analytic procedures are discussed in detail in Chapter 19, covering financial statement analysis.

is that plausible relationships among data may reasonably be expected to exist and continue in the absence of conditions to the contrary." Analytic procedures identify changes in amounts, ratios, trends, or relationships. They may also identify unusual transactions or events.

Analytic procedures are used throughout the audit process for three primary purposes:

1. *Preliminary analytic procedures* are used to develop an understanding of the company and to direct attention to high-risk areas in determining the nature, timing, and extent of audit procedures.
2. *Substantive analytic procedures* are used to obtain audit evidence to evaluate account balances.
3. *Final analytic procedures* are used to assess the propriety of audit conclusions in an overall assessment of the presentation of the financial statement.

SAS 99, *Consideration of Fraud in a Financial Statement Audit,* provides for "considering the results of analytic procedures performed in planning the audit." In addition, analytic procedures that are performed as substantive tests may indicate a previously unrecognized risk of fraud. The SAS recommends specific analytic procedures relating to revenue recognition, a high-risk financial statement item. SAS 99 also introduces the concept of using disaggregated analytics to further address the risk of fraud, especially in the area of revenue recognition. In large, complex companies, even a knowledgeable company executive would be hard-pressed to explain at the consolidated line item level why the numbers are what they are without a more detailed review. Asking the chief financial officer of a global manufacturer why sales increased by 6 percent but cost of sales remained flat, causing an increase in margins over the previous year, may be a question well worth asking—but it would be virtually impossible to sort out all of the causes and effects at the consolidated level.

The more detailed the level of comparison, the more likely that unexpected relationships will surface. Whenever possible, data could be disaggregated and comparisons of the disaggregated data performed. For example, data should be compared by division, by product, by location, by employee, and so on. The smaller the set of data, the less likely that unexpected changes will be minimized, masked, or offset by opposite changes. Also, for analytic procedures to be relevant and useful, consideration should be given to the accuracy and completeness of the underlying sources of the data being used. Such consideration may extend not only to the company's data but also to external data used to generate expectations, though it is not usually necessary to formally test such external data.

Once an auditor has identified the changes in amounts, ratios, trends, or relationships, the next step is to determine whether the changes were expected and, similarly, to determine whether certain changes were expected but did not occur. The need for the auditor to understand the company and its business is evident: The key factors that influence the client's business may be expected to affect the client's financial information. Changes in amounts, ratios, trends, or relationships can be accurately interpreted only in that context. Changes may be due to accounting changes, industry changes such as regulatory changes and changes in the competitive landscape, changes in general economic conditions, strategic changes such as the introduction of a new product or new pricing structure, and other issues such as changes in

personnel. Unexpected changes, or no change when a change was expected, may be due to error, fraud, and sometimes simply to random occurrences.

The passage from SAS 56 cited earlier incorporates several key concepts:

- *Evaluations of financial information* is an expression that suggests that analytic procedures will be used for understanding or for testing financial statement relationships or balances.
- *Study of plausible relationships* implies an understanding of what can reasonably be expected and involves a comparison of the recorded book values with an auditor's expectations.
- *Relationships among both financial and nonfinancial data* suggests that both types of data can be useful in interpreting the financial information and, therefore, in forming an expectation.

The Auditing Standards Board has concluded that analytic procedures are so important that they are required on all audits. SAS 56 requires that analytic procedures be used in audit planning and in the overall review stage of the audit.

In addition to assisting the auditor in detecting fraud, analytic procedures confer other benefits:

- *Assessment of the entity's ability to continue as a going concern.* Conducting analytic procedures may assist an auditor in determining a company's current financial condition, its condition relative to competitors, whether the company is experiencing or may experience financial difficulty, and whether it is able to continue as a going concern.
- *Indication of the possible presence of errors in financial statements.* When analytic procedures reveal differences between a company's actual and expected performance, such differences could represent either accounting errors or irregularities.
- *Implications for audit testing and procedures.* When analytic procedures are performed during an audit and do not reveal differences or inconsistencies compared with expectations, material error or irregularity is less likely to be present. In these cases, it may be possible to perform fewer detailed tests of relevant accounts because the analytic procedures constitute substantive evidence supporting the fair statement of the related account balances. If analytic procedures do reveal differences, additional testing may be required during the audit.

Effective analytic procedures can reasonably be anticipated to identify surprising relationships. Using such procedures, auditors develop expectations for actual financial amounts, ratios, trends, and relationships based on their prior experience of the company (modified to reflect any known factors expected to change the outcome), experience of the relevant industry or of similar companies in the industry, expectations of management at the outset of the reporting period, and the actual operational activities of the company. Therefore, the following comparisons are typical aspects of analytic procedures:

- Current company data versus company data from prior period(s)
- Company data versus company budgets, forecasts, or projections

- Company data versus industry data or comparable company data or both
- Company financial data versus company operational data such as production levels, number of employees, and square footage
- Subset of company data versus other subset of company data: comparison of data on a disaggregated basis such as by division, product, location, or employee
- Company data versus auditor-determined expected results

These comparisons are discussed in more detail in later pages. However, it is important to consider items that are not truly comparable—such as a competitor that uses a different accounting method, a prior period that does not reflect a new product introduction, or a location with demographics that require lower pricing.

Current Company Data versus Company Data from Prior Periods

This procedure includes not only comparing the current period's balance with that of prior periods but also comparing ratios and percentage relationships over time. Comparing only the balances between the two periods would not take into account such factors as growth or the relationship between the financial data. Making comparisons on as small a unit of data as possible—monthly, for example—and for more than just two years will provide additional relevant information. Trend analyses could be performed with monthly data. For example, using analytic procedures to identify fictitious sales entries posted at each quarter's end to meet the quarterly revenue or earnings goals is possible only if data are viewed by periods shorter than a quarter. Graphically depicting these trends may better enable the auditor to determine what needs to be investigated further.

Company Data versus Company Budgets, Forecasts, or Projections

Most companies prepare budgets that reflect their financial performance goals. These budgets are often prepared for various areas within the company—such as departments, plants, and other subunits—and for various activities the organization conducts, such as sales, production, and research. Since budgets represent the client's expectations for the period, differences between actual results and the budget should be analyzed.

Tracking actual to budget from prior periods could be included in the current-year analysis as well. If the company has always had trouble staying within budget, this could be considered. The budget could be evaluated to determine whether it was realistic when prepared. Determining whether the budget was modified during the period to conform to the company's actual financials is also a consideration. The fact that actual amounts approximate budgeted amounts does not necessarily indicate the absence of impropriety. A common fraudulent scheme is to manage the budget to the benefit of either the company or the individual fraudster.

Comparing actual results with analysts' expectations may also provide relevant information.

Company Data versus Industry Data or Comparable Company Data or Both

Company financial data—both balances and relationship data—are compared with data from the whole industry or with that of a competitor or comparable peer. Company performance that differs significantly from industry performance may warrant further scrutiny. Performance measures to be compared with industry measures could include, among others, sales growth, gross profit, net income, bad debt expense, and various ratios.

Company Financial Data versus Company Operational Data

Auditors may consider making comparisons between certain operational activities and the areas of the financial statements that they would expect to be affected as a result. For example, it would normally be expected that increased production levels might appear in the financial statements as increased revenue or increased inventory. Similarly, revenues within units should not exceed total production after adjusting for changes in inventory levels. Other operational data that might be compared with financial data include number of employees, square footage, number of locations, shipping volumes versus volumes invoiced, and other examples relevant to the specific industry.

Company Data versus Auditor-Determined Expected Results

The auditor may have certain expectations for results—such as certain amounts, ratios, relationships, or trends—based on the auditor's understanding of the client and of the industry in which the company operates. A difference between the recorded outcome and the auditor's expectations might indicate a misstatement and require further investigation and corroboration. This analysis is highly dependent on the precision of the auditor's expectation. Generally, the more precise the expectation—that is, the closer the expectation is to the correct balance or relationship, as opposed to the recorded balance—the more effective the procedure will be at identifying potential misstatements.

ANALYTIC TECHNIQUES

As stated earlier, comparisons are made not only on account balances but also on financial relationships. The most common techniques for analyzing relationships are discussed as follows.

- *Horizontal analysis—that is, comparison of the current period's balances with those of prior periods.* This technique calculates the percentage of change between the current-period balance, as well as prior-period balances, and a base period. Accounts that are increasing or decreasing at rates significantly higher or lower than the majority of the account balances—and especially compared with related accounts—might be subject to further scrutiny. For example, if sales increased 22 percent during the base period but the cost of goods sold increased only 9 percent, further analysis of both accounts might be warranted.

- *Vertical, or common-size, analysis.* This technique calculates each line item on a financial statement as a percentage of another line item. An income statement is common sized by showing each line item as a percentage of revenues. This is informative because many expenses, such as commissions or cost of goods sold, are directly dependent on the level of revenues. A balance sheet is common sized by showing each line item as a percentage of total assets—or total liabilities plus equity. These percentages are then compared against prior-period percentages or against industry or comparable company percentages.
- *Comparison of the detail of a total balance with similar detail for the preceding year(s).* This technique is based on analysis of the detail of a specific balance over time or at a point in time and comparison of it to similar detail from prior periods. If no significant changes in the client's operations have occurred in the current period, then much of the detail making up the totals in the financial statements might also remain unchanged. It is often possible to use this method to isolate information that needs further examination. An example might be a detailed analysis of the trade receivables account. Such an analysis could reveal that a significant increase in the number of customers occurred from one period to the next, with most of the new customers having balances below the typical materiality level for performing written confirmations. This might warrant further analysis.
- *Ratios and other financial relationships.* Ratios reflect relevant information about a business by quantifying the relationship among selected items on financial statements. A company's ratios can be compared with ratios from a different period or periods, with a competitor's ratios, and with an industry's ratios. Anomalies in the form of erratic or unexplained changes or differences from the industry may be investigated further. It is instructive to calculate liquidity, activity, leverage, and profitability ratios and figures. Generally speaking, the ratios that may be affected by the four primary fraudulent financial statement schemes include:
  - Current ratio
  - Working capital balance
  - Accounts receivable turnover
  - Inventory turnover
  - Asset turnover
  - Debt or debt to equity
  - Gross margin
  - Operating margin
  - Profit margin

    In addition to those standard ratios, it is also relevant to analyze other relationships involving the high-risk areas of revenue recognition and inventory balances. Relationships that can be analyzed in these categories might include the following:
  - Sales versus sales commissions
  - Sales versus returns, allowances, and discounts
  - Sales versus advertising or promotion budget
  - Sales versus outbound freight costs
  - Sales versus cost of sales
  - Sales versus accounts payable

- Sales versus gross profit
- Sales versus inventory
- Sales versus production levels or capacity
- Sales versus measure of total market size
- Sales versus accounts receivable
- Sales versus interest expense
- Inventory versus cost of sales
- Inventory versus current or total assets
- Inventory versus production levels

Finally, analysis of relationships that involve cash or cash flow can reveal areas requiring further review. The cash account is rarely misstated because of the ease with which cash balances can be confirmed. Therefore, examining the relationship between cash—which is likely to be stated properly—and other account balances that might be misstated can identify anomalies. Some relationships involving cash or cash flow that might be analyzed include the following:

- Cash versus current or total assets
- Cash from operations over time
- Cash from operations versus sales
- Cash from operations versus net income
- Free cash flow (operating cash flow minus capital expenditures and dividends)

It is generally appropriate to use more than one of these comparisons or relational techniques or both because different techniques may reveal different information. Unexpected relationships should be considered for further analysis. For example, if operations are financed with a working capital line and production and sales are up but interest expense is down—assuming no decline in interest rates—further analysis may be warranted. It may be that other efficiencies facilitated cash flow from operations to be used for financing the increased production and sales, or it may be that fictitious sales were booked.

ASSESSING THE POTENTIAL IMPACT OF FRAUD RISK FACTORS

SAS 99 makes clear that the auditor must apply professional judgment not simply in determining that there is a theoretical risk of material misstatement due to fraud but also in "the consideration of the attributes of the risk, including:

- The *type* of risk that may exist: whether it involves fraudulent financial reporting or misappropriation of assets
- The *significance* of the risk: whether it is of a magnitude that could result in a possible material misstatement of the financial statements
- The *likelihood* of the risk: the likelihood that it will result in a material misstatement in the financial statements
- The *pervasiveness* of the risk: whether the potential risk is pervasive to the financial statements as a whole or specifically related to a particular assertion, account, or class of transactions"[22]

[22] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, pars. 35–40.

All of these attributes will influence both the extent to which the auditor needs to take specific steps to respond to a particular risk factor and the nature of those steps.

The range of possible responses is considerable. At one end of the spectrum, the auditor may reasonably conclude, after proper consideration of the foregoing attributes, that no specific steps need be taken. At the other end, the auditor may have such grave concerns and therefore may feel unable to form an opinion. The auditor may even consider resigning the appointment.

All but one of the foregoing attributes are simply more sophisticated statements of the common, intuitive risk formula: probability multiplied by downside. The exception is *type,* which has no direct bearing on either the probability or extent of a potential misstatement but has significant impact on the nature of the response to a particular risk. For example, the auditor's approach to addressing the risk of material misstatement resulting from intentional overestimation of the value of an asset in a highly judgmental area may be quite different from the approach taken to the risk of material misstatement arising through the concealment of theft of physical inventory.

The likelihood or probability of a material misstatement due to fraud cannot be precisely quantified. An auditor's assessment of this attribute may be influenced by a personal assessment of the entity's internal controls (including the existence of an effective audit committee or other supervision of management)—in particular, the effectiveness of internal controls designed to deter or mitigate the risk in question. In any event, in keeping with the need to apply professional skepticism at all times, the auditor should not base an assessment of likelihood solely on a general belief in the integrity of management or others or on the fact that material misstatements due to fraud occur relatively rarely.

The attributes *significance* and *pervasiveness* are closely related; both address the potential scale of the misstatement that might arise. A risk is significant if it could potentially lead to a material misstatement in the financial statements. The pervasiveness of a fraud risk factor has to do with whether that risk threatens the accuracy of the financial statements as a whole or threatens only specific assertions, balances, or transactions. It is not necessary for both attributes to be present for there to be a risk of material misstatement. Naturally, in assessing whether a material misstatement could arise, the auditor should consider the impact on both the balance sheet and the profit-and-loss account. A deliberate overstatement of inventories may not be material in balance sheet terms but could nonetheless be material with regard to profit.

EVALUATING CONTROLS

SAS 99—in conjunction with SAS 55,[23]—requires the consideration of internal controls as the final ingredient in the assessment of identified risks of material

[23] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 55, *Consideration of Internal Control in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 319).

misstatement due to fraud.[24] On one hand, effective controls may mitigate a particular risk of material misstatement due to fraud. On the other hand, deficiencies in control may have the opposite effect, actually exacerbating the risk.

The potential benefit of this step is that the identification of effective controls, which genuinely mitigate a particular fraud risk, may provide the auditor with a reasonable basis for concluding that the likelihood of that kind of fraud is low. Such an assessment will be taken consistent with SAS 55 and any other relevant standards and only once the auditor is comfortable relying on the relevant controls.

Reliance on controls in specific instances does not obviate the need to consider the possibility of management override. SAS 99 suggests a number of procedures that "should be performed to further address the risk of management override of controls."[25]

- Examining journal entries and other adjustments for evidence of possible material misstatement due to fraud
- Reviewing accounting estimates for biases that could result in material misstatement due to fraud
- Evaluating the business rationale for significant unusual transactions

Using the fraud triangle (incentive or pressure, opportunity, and rationalization or attitude) as a framework, the auditor considers whether there is evidence of other fraud risk factors. The auditor also considers the possibility that collusion, which might lead to the circumvention of controls, is occurring at other levels of the organization. For example, a control over purchases involving segregation of duties between the staff member responsible for opening supplier accounts and the staff member responsible for processing invoices may be overridden if the two individuals collude so they can establish an account and process invoices for a fictitious supplier.

In addition to SAS 99, the PCAOB's AS2 specifically requires that the auditor consider antifraud programs and controls. Common elements of an antifraud program to be assessed include:

- Code of conduct
- Ethics hotline or whistle-blower programs and activities
- Hiring and promotion
- Audit committee
- Oversight
- Investigation and remediation
- Fraud risk assessment

While some of these common elements may be evaluated for the effectiveness of internal controls as part of the five key components of COSO (see Chapter 6), this requirement is separate from that internal control evaluation because it focuses on the risk of fraud.

[24] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, pars. 43–45.
[25] Id., par. 57.

Addressing the Identified Fraud Risks

The identification and evaluation of fraud risk factors, discussed at some length here, constitutes only the beginning. On the basis of their evaluations, auditors determine how best to address identified fraud risks to obtain reasonable assurance as to whether there is, in fact, any material misstatement due to fraud in the financial statements that are the focus of the audit. The auditor's actions may include:

- Considering the level of supervision of personnel to ensure that it is "commensurate with the auditor's assessment of the risks of material misstatement due to fraud"[26]
- Reviewing management's selection of accounting policies: When a heightened fraud risk is evident, the auditor should review the accounting policies and procedures adopted by management—especially in areas subject to significant uncertainty or judgment—and consider whether these might be applied or misapplied in such a way as to result in material misstatement
- Incorporating an element of unpredictability into the audit approach—for example, (1) including within the scope of audit testing certain balances or transactions that are not normally included, (2) visiting locations without advance warning, or (3) changing the timing or scope of audit tests
- Considering more generally the nature, timing, and extent of audit procedures with regard to their effectiveness in addressing the risk of material misstatement due to fraud

UNPREDICTABLE AUDIT TESTS

Opportunity is one side of the fraud triangle. Predictability of the audit approach may create opportunity and undermine detection. As such, unpredictability may be adopted as a strategy on two levels. At a high level, the auditor may decide to visit locations or to audit areas of the business or components of the financial statements that are not normally audited in detail or at all. If all areas are normally subject to audit by rotation, the auditor might deviate from the expected sequence. At a more detailed level, the auditor should be wary of being too predictable in the selection of individual transactions for detailed testing and avoid situations in which the client might have the opportunity to influence the selection or to manipulate audit evidence.

In one case, auditors in a company failed to detect material misstatements in the financial statements for a six-year period because all of the fictitious transactions—and there were many—were either below scope or with business partners who consistently failed to respond to confirmation requests. The perpetrators were armed with the knowledge of what scope the auditors consistently used and which entities consistently failed to respond to confirmation. The perpetrators were able to deceive the auditors and all other third-party users for an extended period of time. In another case, it was alleged that the company knew that its external auditors examined fixed-asset additions at any given facility only if those additions

[26] Id., par. 50.

exceeded a certain value. In manipulating fixed-asset additions—an integral part of the alleged financial reporting fraud—the company was careful not to exceed that dollar threshold at any single facility, thereby circumventing the audit process. These examples speak to the importance of modifying the audit approach over time.

Paragraph 50 of SAS 99 specifically states that "the auditor should incorporate an element of unpredictability in the selection from year to year of auditing procedures to be performed." Modifications, either selected randomly or focused on the higher-risk areas, might include:

- Testing areas or accounts that might not normally be tested by the auditors
- Performing substantive tests in areas that have been sampled previously
- Changing sampling methods or increasing sample size
- Obtaining confirmations when, historically, none have been obtained
- Obtaining oral confirmations when, historically, only written confirmations have been obtained
- Performing physical observations in areas in which, historically, only documentary evidence has been reviewed
- Performing procedures at different locations
- Conducting unannounced observations or tests
- Changing the timing of test work
- Modifying the materiality level for certain accounts, testing selected items that are under the materiality level, or testing selected items that are not normally tested because they are considered to be low in risk
- Making inquiries of individuals not approached in previous audits
- Incorporating unpredictable procedures in the testing of journal entries, such as randomly selecting immaterial entries for testing

The point is neither to adopt new overall procedures—such as switching from written to oral confirmations—nor to make a onetime change in procedures. The point is to continually modify the approach so as to make it unpredictable. Not only could this aid in detecting fraud, but it also may serve as a fraud deterrent.

OBSERVATION AND INSPECTION

As mentioned earlier, indications of fraud risk can emerge at any stage of the audit, and the auditor should be alert to events or circumstances that may call for revisions in the previous assessment of fraud risk. There is no substitute for physically and manually reviewing documents, data, and assets. Observation and inspection are standard parts of any audit work program, including vouching and tracing and performing or observing physical counts. Substantive anomalies may come to light through these testing procedures, such as implausible transactions or financial ratios and relationships, or what might be called evidential risk factors may come to the auditor's attention. SAS 99 cites the following examples:[27]

[27] Id., par. 68, examples cited in full.

- Discrepancies in the accounting records, including:
  - Transactions that are not recorded in a complete or timely manner or are improperly recorded as to amount, accounting period, classification, or entity policy
  - Unsupported or unauthorized balances or transactions
  - Last-minute adjustments that significantly affect financial results
  - Evidence of employee access to systems and records inconsistent with the access necessary to perform authorized duties
  - Significant unreconciled differences between control accounts and subsidiary records—or between physical count and the related account balance—that were not appropriately investigated and corrected on a timely basis
  - Tips or complaints to the auditor about alleged fraud
- Conflicting or missing evidential matter, including:
  - Missing documents
  - Unavailability of other than photocopied or electronically transmitted documents when documents in original form are expected to exist
  - Significant unexplained items on reconciliations
  - Unusual documentary evidence such as handwritten alterations to documentation or handwritten documentation that is ordinarily electronically printed
  - Inconsistent, vague, or implausible responses from management or employees arising from inquiries or analytic procedures
  - Unusual discrepancies between the entity's records and confirmation replies
  - Missing inventory or physical assets of significant magnitude
  - Unavailable or missing electronic evidence inconsistent with the entity's record retention practices or policies
  - Inability to produce evidence of key systems development and program-change testing and implementation activities for current-year system changes and deployments
- Problematic or unusual events between the auditor and the client, including:
  - Denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought
  - Undue time pressures imposed by management to resolve complex or contentious issues
  - Complaints by management about the conduct of the audit or management intimidation of audit team members, particularly in connection with auditors' critical assessment of audit evidence or in the resolution of potential disagreements with management
  - Unusual delays by the entity in providing requested information
  - Unwillingness to facilitate auditor access to key electronic files for testing by means of computer-assisted audit techniques
  - Denial of access to key information technology operations staff and facilities, including security, operations, and systems development personnel
  - Unwillingness to add or revise disclosures in the financial statements to make them more complete and transparent

When comparing sources of audit evidence, such as comparing invoices with the accounts payable ledger or comparing bills of lading with inventory entries, the

auditor does not simply locate the amount either on the document or in the books and records but reviews the source document with a critical eye for issues such as the following:

- Is the booked amount the correct amount? For example, are shipping and freight also included?
- Does the date of the document reflect the posted date of the transaction, and does it make sense given other dates such as the order-placed date?
- Do the terms—discounts, returns, and so on—reflect actual events?
- Does the document look legitimate?

Other questions may also apply.

Fake or altered documents often have certain characteristics, depending, of course, on the perpetrator's level of sophistication. Here are some examples:

- Font sizes or types may not be consistent.
- No address is shown for the vendor or customer: This is especially suspicious if a vendor has not identified an address to which a check can be sent.
- The address shown is a post office box rather than a physical address.
- The document has no identifying numbers such as invoice number, purchase order number, or customer number.
- All invoice numbers—on invoices from vendors—are numbered sequentially, with no numbers skipped.
- No tax is shown for taxable items.
- No shipping or freight is shown for items that would have been shipped at the purchaser's expense.
- No detail is provided on the invoice.

The presence of these or similar characteristics may suggest the need for further analysis.

As indicators of the possible existence of fraud—whether fraudulent financial reporting or misappropriation of assets—such evidential potential red flags may be considered to have a different status from the general fraud risk factors that have been the topic of most of this chapter. While evidential potential red flags are, like general fraud risk factors, not in themselves conclusive evidence of fraud, they do indicate the existence of a specific gap, anomaly, or other problem in the available audit evidence. As such, they require follow-up.

FINANCIAL STATEMENT FRAUD: DETECTION TECHNIQUES

Knowing where to look for fraud is a key component in detecting fraud.[28] While any line item on the income statement or balance sheet is subject to manipulation, this happens more regularly in certain areas. The auditor should be most alert to potential schemes affecting these line items. Thinking about potential schemes can assist with risk identification. Most often, the goal of fraudulent financial reporting is to overstate net income or net worth—although the opposite may be true when

[28] Part of knowing where to look lies in understanding how a fraudster thinks. This is discussed in Chapter 3, "Psychology of the Fraudster."

individuals are engaged in earnings management and in building the stockpile of reserves during profitable years to be used later, during periods of lower financial performance. For net income to be overstated, revenues typically are overstated or expenses typically are understated or both. For net worth to be overstated, assets must also be overstated or liabilities must be understated or both. In the system of double-entry bookkeeping, any inappropriate entry will appear in two or more line items. The auditor should understand the client's risk identification program; not having such a program raises a potential red flag.

REVENUE RECOGNITION

Fraudulent financial reporting by means of improper revenue recognition is one of the most prevalent forms of material misstatement due to fraud. For this reason, SAS 99 stipulates that the auditor "should ordinarily presume that there is a risk of material misstatement due to fraud relating to revenue recognition."[29] SAS 99 goes on to discuss examples of procedures for addressing the risks related to revenue recognition.[30]

The auditor considers the nature of the entity's business and how it generates and accounts for revenues and then identifies ways in which revenues might be misstated and how such misstatement might be concealed. Examples of the specific risks the auditor might consider, depending on the nature of the business, include the following:

- Fictitious sales of tangible goods might be created and concealed by the falsification of inventory records, shipping documents, and invoices.
- Sales might be inflated by the shipping of goods not ordered, by treating consignment shipments as revenues, or by otherwise ignoring shipping terms that deal with ownership transfer.
- Fictitious sales may be booked for product that has been packaged but not shipped to the customer—and will never be shipped. The sale may be written off later or re-aged so as not to adversely affect ratios and metrics.
- Sales might be subject to side agreements giving customers the right to return goods not used or to other arrangements that have the effect of partially or wholly reversing sales.
- Sales cutoff might be manipulated by holding the books open for a period after the year-end.
- Fictitious or inflated revenues from long-term projects in progress might arise as a result of aggressive estimates as to degree of completion. This risk will tend to be increased when significant judgment is required in measuring the value of work done or the state of completion—for example, in relation to large-scale capital projects or the development of intangible products such as custom software.

[29] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, par. 41.
[30] Id., par. 54.

Indicators of such manipulation might include but are not limited to unusual sales patterns or ratios emerging from analytic procedures, discrepancies in documentation, recognition of revenues not in accordance with the contract, large credit notes after the year-end, long-outstanding debtors, unreconciled debit entries on intercompany accounts, or irregularities in inventory counts. It is important to obtain a thorough understanding of significant revenue sources and related revenue recognition policies, as well as of any recent changes.

CORRUPTION

Detection of bribes and kickbacks is difficult at best because these are typically buried in otherwise legitimate transactions. That is, the company usually overpays for goods and services, whereupon the perpetrator receives a kickback from the vendor representative. As such, bribes and kickbacks generally involve the purchasing function of the organization. Potential targets of such schemes include anyone with authority to award contracts or to purchase products—such as inventory, supplies, raw materials, fixed assets, and software. Potential targets may also include individuals whose sign-off is needed for acceptance of a contract, such as engineers, quality personnel, and other technical experts.

Since corruption frauds are so difficult to detect, the focus is weighted heavily toward deterrence. Controls need to be exceptionally good in this area to mitigate the risk that these transactions will occur in the first place. Deterrence may begin by assessment of the areas in which control weaknesses exist. Some excellent control mechanisms are as follows:

- Integrity in the asset procurement bidding process
- Rotation of employees through various vendor assignments
- As a way of deterring the perpetrator from informing a partner about lower-bidding competitors, the use of private fax machines whereby bids are required to be submitted to persons other than those soliciting the bids
- Establishment of a hotline and ensuring that vendors are aware of the hotline and encouraged to use it if any employee approaches them, seeking a bribe
- A strong, enforced policy on disclosure of conflicts of interest, including receipt of gifts and gratuities by buyers

As with the other types of frauds, analytic procedures and data mining may assist in detection. The typical result of a corruption scheme is that the victim company overpays for a product or service. Trending expenditures and then analyzing the reason for any increases or failures to decrease when a declining trend was expected may identify the purchase of unneeded items or of necessary items at inflated prices. Trending asset balances may also reveal the purchase of unneeded assets, including inventory. Excess inventory write-offs may be the result of a fraudster's attempt to make room for additional purchases. Other potential red flags that may indicate a possible corruption scheme include:[31]

[31] Association of Certified Fraud Examiners, *Fraud Examiners Manual,* 3rd ed. (Austin, TX: Association of Certified Fraud Examiners, 1998).

- Orders consistently placed with the same vendor
- Cost of materials or other purchases out of line when compared with related activities
- Buyers whose lifestyles appear to exceed their income levels
- Procurement decisions—in favor of key suppliers—that are heavily influenced or made by managers outside the purchasing department
- Restrictions in solicitation documents that tend to restrict competition
- A very short timeframe for responding to bids

SUMMARY

SAS 99 lays out an iterative and holistic approach to the consideration of fraud in a financial statement audit, the foundation for which is a proper attitude of professional skepticism. The planning, testing, and evaluation of audit evidence for indicia of fraud are unlikely to be successful without that attitude, particularly because fraud is a crime of deceit and because the popularly labeled potential red flags, which may appear by hindsight as bright-red flags, are more like mere threads in their true contemporaneous context. Nevertheless, armed with attitude, analytic techniques, an appreciation of the interpretive challenges presented by fraud risk factors, and the benefit of experience, auditors will continually improve the detection of fraud that materially misstates financial statements.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 14

Investigative Techniques

Mona M. Clayton

This chapter is a toolbox. While many preceding chapters have discussed investigative techniques in the context of other topics (see Chapter 13 in particular), we have not yet opened a number of trays in the toolbox. The chapter also looks at the administrative issues surrounding forensic accounting investigations, which require knowledgeable management. In any specific circumstance, some tools will be more useful than others in the effort to generate investigative results that can withstand scrutiny by the client, legal counsel, and regulatory and judicial authorities, not to mention quality and risk management reviewers in the forensic accounting investigator's own firm. All of the tools have their place and purpose. We begin with the administrative issues and then go on to specific techniques.

TIMING

While audits are usually predictable in their timing and fieldwork, most investigations are not. On one hand, with few exceptions auditors know their client commitments 6 to 12 months in advance, and clients know what to expect of their auditors over the same time horizon. On the other hand, forensic accounting investigators often enough cannot anticipate their client commitments even two weeks in advance, let alone six months in advance. It is not unusual for them to receive a call on a Friday afternoon and, in response, over the weekend deploy a team to a distant location in time for the opening of business on Monday.

Pending filing deadlines may affect the timing, priority, and sequence of investigative procedures. Investigating can be a lengthy process due to the volume of data requiring review. Transaction review takes time, document review takes time, e-mail review takes time. Investigative leads may take the team into areas not contemplated at the outset of an investigation. Yet all of this is normal. Discuss these issues with the client, audit committee, or counsel to determine the priority and sequence in which existing and new issues should be addressed.

Having a plan and working to that plan structures the engagement. A looming deadline is rarely a good reason to trim procedures and back away from a thorough investigation as initially planned. Stand firm on quality. Communicate timing of proposed scope changes and proposed fees early and often to avoid surprises for the client and investigative team.

COMMUNICATION

While communication sounds as if it is a basic and well-understood aspect of conducting an investigation, it should not be taken lightly. Effective communication, including setting clear expectations, is an essential skill of the investigative team. Working for and with various parties, ranging from audit committees to outside regulatory bodies, the forensic accounting investigator's communications are, in fact, critical. More than one master may be needed for those communications, including the risk management group and legal counsel at the forensic accounting investigator's own firm, audit partners, consulting partners, other accounting firms, outside legal counsel, prosecutors, the U.S. Federal Bureau of Investigation (FBI), management, inside legal counsel, compliance, and internal auditors—and this roster of possible stakeholders is not necessarily complete for any given circumstance.

Clear, frequent, and timely communications are necessary. Unanticipated complications can often occur when communicating with international multicultural teams and across multiple time zones. Whether you're dealing with language barriers, cultural assumptions, or the simple mechanics of a conference call, leave nothing to chance. This cannot be stressed enough. The absence of clear, frequent, and timely communications can result in misunderstood time lines and deadlines, missed conference calls, dissatisfaction, even fee disputes. If in doubt, communicate. Even if not in doubt, communicate.

EARLY ADMINISTRATIVE MATTERS

The following administrative concerns usually come up early in the process of setting an investigation in motion and remain important throughout:

- *Relationship review and conflict check*. This process identifies the entity and party names to be compared with outstanding engagements. Potential conflicts should be cleared, calls made, and responses documented before accepting the engagement. Usually, the names of the parties are obtained from the person, such as an attorney, who requests your services. For some potential clients, additional research or vetting may be needed—for example, by obtaining a Dun & Bradstreet report, calling a foreign office, or reviewing public records to determine the viability of the entity. Retainers may be obtained and applied to the final billing to offset potential risks that may show up through this qualification process. For firms with international locations, additional vetting and communications may be required to understand any services that were performed in another region.
- *Engagement letter*. The engagement letter is likely to vary by firm and to include various elements. At a minimum, it would normally include the name of the client, the scope of services, fee arrangements (which may include a retainer), and, perhaps, indemnification and reference to legal matters. On engagement letters, consider obtaining signatures from legal counsel as well as the ultimate client who is paying the fees. Note that for existing external audit or internal

audit clients, an addendum to the existing engagement letter, outlining additional scope and fees, may be sufficient. The process may vary, depending on the firm's risk management protocol.

- *Billings and fees.* Strive to keep the client aware of fees incurred and outcomes. You do not need to wait until a bill is sent on your firm's normal billing cycle to inform the client of a fee estimate or fees incurred. Some clients do not balk at fees, while others do. You may prefer to communicate fees in phases or by the week or day or professional. The level of detail depends on your own firm's business practices and the preferences of the client. Based on priorities, the client may opt to delay some tasks or perform them through in-house resources, once the time and expense associated with the tasks have been communicated.

PREDICATION

The investigation may begin with a telephone call from a concerned client or audit committee chair. There may be allegations in an anonymous letter or a suspicion of fraud uncovered by an audit team. From whatever source, there are allegations, and the party contacting you has decided that it would be an error to ignore the allegations.

All valid reasons to contemplate launching an investigation can be categorized as *predication.* According to the *Fraud Examiner's Manual*, predication is "the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, or will occur. Predication is the basis upon which an examination is commenced. Fraud examinations should not be conducted without proper predication."[1] Anonymous tips, complaints, and audit inquiries may surface predication meriting further inquiry. Furthermore, predication can be identified by a number of sources, including but not limited to external auditors, internal auditors, management, employees, third parties, and regulators.

The following examples of predication should not be viewed as a comprehensive listing, but they suggest the various forms that predication may take.

Responding to Regulatory Action

- The SEC has initiated, or a knowledgeable party anticipates that it will initiate, an informal inquiry into certain issues, and our company wants to be able to respond effectively.
- The company is undergoing a 10A investigation.[2] What must it do next?
- The local regulator that monitors price fixing and cartels raided our company yesterday.

[1] Association of Certified Fraud Examiners, *Fraud Examiners Manual* (Austin, TX: Association of Certified Fraud Examiners, 1998).

[2] See fn. 6 in Chapter 5 regarding 10 A and its reference to the independence of the external auditors.

Difficulties in Financial Reporting and Information and Disclosure

- We cannot seem to get timely and accurate reports from [a person, department, location, division, subsidiary].
- We made an investment in [location or product], and the early performance reports are troubling despite our up-front due diligence efforts.
- Our internal audit or operations team has just returned from a visit to [location] and reports serious discrepancies.
- There may be a problem with the accounting for [issue]. We want you to take a look at the accounting process and treatment in certain locations and give us your assessment. We are unsure of the impact on the financial statements and the possible need for a restatement.

Issues Involving Customers or Vendors

- Our [department or location] manager seems to insist that we use a certain vendor. That strikes us as a red flag.
- We noticed that a new customer made a $300,000 purchase this month, but we cannot reach anyone at the entity. Could you conduct a public records search and tell us what you find?

Matters Relating to the Foreign Corrupt Practices Act

- We are doing business in [location], and we are concerned that bribes, kickbacks, or unwarranted commissions are being paid to conduct business there.
- We have just completed an investigation in [location], which surfaced some FCPA issues, and we would like you to perform similar procedures in [location].
- We are contemplating an acquisition in several emerging markets and need forensic accounting specialists to perform FCPA or antibribery and corruption due diligence.
- As part of our efforts to improve our compliance program, we need some assistance to assess our compliance risk in regard to FCPA or antibribery and corruption.

Lifestyle

- Our [title of individual] just left for a vacation in [super luxury location] and has been acquiring possessions that exceed his expected lifestyle.

Anonymous Tips

- Our [division, location] always hits the numbers, but we have received an anonymous tip that something is wrong there.
- Our [high-level executive] just resigned or died unexpectedly. We have heard rumors and want you to come in and talk with some of our employees.

Conflicts of Interest

- One of our employees was watching late-night television and saw a commercial for a new restaurant in town. The restaurant owner is one of our plant general managers.
- We've heard rumors that our operations manager is an officer of a temporary services company that provides employees for our warehouse. We have paid this entity $1.5 million in the past nine months. Our employees are required to disclose potential conflicts of interest, but we do not have a disclosure from this operations manager. We would like to take a look at all areas for which this person is responsible, and we want to know about the person's real or potential undisclosed conflicts of interest.

Obviously, the list could continue. The intent is to illustrate that predication takes many forms.

WHAT SHOULD YOU KNOW BEFORE YOU START?

Assuming that you are in a position to accept the engagement to which you have been alerted, you will need answers to many questions. A basic understanding of the issues is key to planning and gathering the right resources so you can better execute whatever procedures you select from the toolbox. The questions that follow may not generate direct and immediate answers, and not all of them will be suitable to the circumstance. There may be other questions of importance not listed here as well. However, consider the following partial list of typical areas of inquiry, and remember that some of them may be brought up again after the fieldwork begins.

Gaining an Understanding

- *What is the timeframe under analysis?* The client may elect to start with a certain time period and then progress the investigation forward or backward, depending on the results of the initial assessment.
- *What is the nature of the concerns or allegations?* Obtain a complete understanding so as to identify individuals to interview and documents to secure or obtain.
- *Where is the site, and what are the logistical demands to work there effectively? Do we have the necessary linguistic skills if the site is in a foreign country? How can we leverage our presence in the local office or market to support this engagement? Who is our contact at the location?* Obtain details of the locations and names of liaisons at the locations. In remote or foreign locations, the names of hotels and landmarks can be helpful. For foreign travel, visas may be required and for some countries there may be concerns about security. Using local contacts and resources is encouraged. This can bring efficiencies to the engagement and avoid blunders such as scheduling fieldwork during a holiday.
- *Who are the targets?* Based on the predication, determine the potential targets of the investigation. The client may have taken disciplinary action prior to engaging

you, perhaps by terminating personnel or putting them on administrative leave. Obtain information about any employment disputes and other relevant history, as well as security concerns.

- *What type of deadlines, reporting requirements, audit committee meetings, and the like are pertinent to the investigation?* These milestones may affect the timing and scope of the investigation and the sequencing of tasks.
- *Have other investigations of the focus issues been conducted at this location?* If so, obtain the reports or an understanding of the findings.
- *What other entities, regions, or sites may be involved? Is the conduct isolated or widespread?* When asking these questions, you may discover, for example, that the general manager under scrutiny also recently managed a different geographic area for the company. The question may identify other at-risk locations to include in the investigation. Do not assume the conduct is isolated without a proper evaluation.
- *Are background checks of employees conducted as a precondition of employment?* If so, request the information or consider updating the information or both. If not, consider performing public records searches for entities or individuals pertinent to the investigation. (See Chapter 15.)
- *How long has the problem apparently existed? Does it predate any of the key current players?* Depending on whom you ask, you may receive different answers to this question. It may be within the scope of the investigation to resolve the discrepancies in responses to this question. Persistence and attention to detail are key.
- *Is there an employee, vendor, or customer with a personal or family problem or an addiction (drugs, alcohol, gambling), who might seek additional financial resources at any potential cost and risk?*
- *Is this an industry or location that has a history or culture of corruption?* If so, gaining an understanding of common industry or culturally tolerated schemes and scams may enhance your ability to evaluate risk and scope. Obtaining local insight is prudent, particularly if evaluating a situation outside your home country.
- *Has the entity been in compliance with reporting and regulatory requirements?* Regulatory requirements may be at multiple levels with various government entities and regulators. After understanding the facts, a fraudulent scheme may also have a tax impact. In some countries the tax impact(s) can be complicated and requires tax specialists to perform the evaluation.
- *What is the profitability of the entity? Has it hit its targets? Has it been adversely or positively affected by industry trends or the general economy? If the entity is meeting or exceeding expectations, does that make sense in light of industry trends and the economy?* There have been pressures placed on emerging markets to produce a larger share of company profits. These pressures can lead to an increase of financial statement fraud. This type of fraud may go undetected for a period of time due to: (a) the lack of statutory audits or external audits or both in these growing businesses, and (b) the lack of financial and fluctuation analysis because the entity may not yet be material to the overall company.
- *What level of growth or decline has the company had, and how does that compare with the growth or decline of its industry and peers?* Ask yourself, "Does this make sense?"

- *Do you know about local management and key personnel?* Understand the payments inuring to local management, on international matters. This applies to general managers or ex-pats on assignment. Managers may have an incentive to misstate financial results for their own benefit. How long have key local managers been in place? Has any due diligence of public record searches been performed on local management? Does local management or a key employee have an undisclosed interest in another entity or entities? Some of these issues may be common in emerging markets because of a lack of transparency.
- *If there has been a recent acquisition, is former management still in place? If yes, is there an earn-out provision in effect?* If so, management may have a large incentive for achieving certain financial measures. Such measures can be achieved honestly—or by fraudulently manipulating a few journal entries or postponing updating estimates. New acquisitions usually have pressure to produce results, thus increasing the risk of bribery and corruption related to obtaining and retaining business.
- *Does the company have a fraud policy? An annual conflict-of-interest policy or attestation?* If so, consider obtaining the attestations of certain individuals if these issues are part of your investigation. Understand company policies concerning conflicts of interest and ethics. Are employees aware of company policies? Are employees required to disclose related-party interests?
- *Does the company have a hotline? Does the hotline have multilingual capacity and access? Is it available to third parties? Do employees know that it exists? Do they conduct training on fraud awareness and antibribery and corruption topics?* If yes, inquire about past hotline communications to identify if there are trends and prior issues. In emerging markets, it is common that items that are commonplace with a basic compliance structure will be lacking, including policies, hotlines and training. Management in Western markets may have a false sense of security regarding the adequacy of their compliance program in emerging markets, as it is common that many employees without management titles will not be aware of these basic compliance measures.

Gathering and Securing Information

It is imperative to maintain control of documents requested and received. Documents may be obtained in many forms, ranging from paper to electronic. Requesting, obtaining, and maintaining document control are usually important aspects of any investigation. This task should not be taken lightly, especially in cases in which there are thousands, if not millions, of documents, and binders and boxes may be in the hundreds.

- *What information can I obtain before the field visit?* The information may include organizational charts, alleged smoking-gun documents, electronic files, personnel listings for potential interviews, financial statements, operational statements, public filings, public records searches or corporate intelligence, press releases, blogs, and Internet postings (stock chat rooms). If there were anonymous tips, complaints, or letters, now would be the time to obtain them.
- *Is there information that should be secured in advance of the field visit?* The client may need to secure or obtain backup tapes, computers, or network data

to avoid destruction of data after your arrival. Now is the time to involve the forensic technology professionals to ensure that the correct information is obtained in the right way the first time around. Doing so probably will prevent rework and incomplete data sets. A visit may also be scheduled to review the offices and files of certain employees. Consider if there are data from handheld devices that should be preserved.

- *Are the audited and statutory financial statements available for analysis?* Obtain the financial statements and management letter comments. For offsite locations, confirm whether the corporate office ever received its financial statements, management letter comments, or internal control observations and recommendations. Sometimes there are different firms that conduct statutory procedures in foreign locations, creating a disconnect with reporting and communications.
- *Are the auditor's working papers available for review?* The client usually assumes that the work papers will not be made available for review or access. The request is worth making, however, and you may be pleasantly surprised by the cooperation you obtain. Releases may need to be signed before reviewing the work papers of other firms. Coordinate with your office of general counsel to ensure that the correct protocol is followed in these situations. Scheduling discussions with the outside auditors can sometimes be arranged without difficulty when the proper protocol is followed. Remember here, too, that clear communication is your friend.
- *Are there internal audit reports available for review? What about reports from compliance, security, legal, due diligence, compliance, risk management, or ethics personnel?* Sometimes investigations may be conducted by departments other than internal audit. Also, there may be preliminary reports or findings that have been made available to the audit committee, special committee, ethics committee, compliance office, and so on. Ask for all reporting—formal or informal—to and from these groups.
- *Is e-mail available for analysis?* If analysis of e-mail and user files is within the scope of the investigation, the files may need to be secured prior to the arrival of the team in the field. A specialist may be needed to obtain and copy or image network files, backup tapes archives, and files on PCs or desktop computers and to prepare them for analysis. Consider the language skills needed for analyzing the e-mails and documents.
- *Are there PCs, laptops, servers, or any other electronic devices that need to be secured?* Identify the particular computers, and consider when to sequence the imaging of the machines in the investigative plan. Some clients may opt to delay this process until after initial scoping is completed, so as to determine whether copying the computers is warranted. Note that there is a difference between copying a hard drive and imaging a hard drive. A forensic image of a hard drive is more complete than a copy. Without imaging technology, deleted and encrypted files may be ignored. A recent investigation found deleted files and 18,000 deleted e-mails that had been deleted just hours after the suspect learned that his computer was to be obtained as part of an investigation. Without imaging, this information would never have been found. (See Chapter 17 for more information on this topic.)
- *What public records searches or corporate intelligence should be conducted?* It may be useful to obtain the names of entities (customers, vendors, and so forth)

and to conduct public records searches before the field visit, if those names appear in the predication or allegations. Performing a public records search before the field visit may yield valuable information, such as knowing whether any employees are undisclosed officers of key suppliers. Keep in mind that public records searches in some countries may take longer than you expect. The legality of conducting searches and the ability to do so are likely to differ across legal jurisdictions. Obtaining permission from the company's general counsel before proceeding is always recommended.

- *Where are documents and computerized records?* The client location may be in Idaho, while disbursements may be processed in India. You may encounter different locations for different records, depending on what you are seeking. Voucher packages for prior years may be in offsite storage, and a service provider may be used to archive e-mails and computer files. Outsourced providers may be used for payments processing. Request computerized information to conduct data mining and analysis. Obtaining and analyzing certain information in these categories may be useful before the field visit. If the client site has been recently purchased or sold, the records for prior years may exist at another entity.
- *Was there a computer system change during the period under analysis?* Determining this item may answer your questions on the time period under review. However, obtaining information from predecessor systems or prior owners or both may be difficult. (See Chapter 17.)
- *What third parties should be considered for interview, contact, or confirmation purposes?* This category may include former employees, vendors, customers, or competitors. There may be some pressure from the company not to extend inquiries out to third parties, owing to a concern that the external inquiries will be disruptive. However, forensic accounting investigators should not retreat from planned and relevant inquiries, even if the inquiries raise initial concerns of this kind. They need to communicate effectively the importance of the external inquiries. After consideration, many companies are often willing to experience some level of uncertainty along the path to resolving allegations. Obviously, if your client does not agree to such contacts, you should not perform them.
- *Have the authorities been contacted? Do you know how to handle the media?* Local police, regulators, prosecutors, the FBI, banking officials, and news media all may play some role in the inquiry. At some point in your career, you may find yourself investigating a high-profile situation with daily, if not weekly, coverage in the business press. If the press contacts you, consult with your office of general counsel, as well as a public relations professional, to determine whether making a statement is appropriate. Remember that nothing is really off the record, reporters' assurances notwithstanding.

Coordination

How often should the investigative team communicate internally? The desirable frequency of teamwide communication depends on the situation. For fast-moving assignments with large teams, you may need to coordinate frequent conference calls among the team members. The team may include internal as well as external members. If in doubt, communicate.

Other

- *Should your investigation be conducted in phases with appropriate checkpoints regarding timing and fees?* Obtain confirmation, in writing, of any changes in scope during the course of the engagement. Obtain an understanding in advance regarding whether a written report will be required and whether a certified translation of the report is required in the local language, regarding the degree of formality required, and regarding who will be the ultimate users of the report.
- *What reports, written or oral, does the client expect?* Reports take time and cost money, and they may be discoverable. Caution should be exercised if you are requested by the client to quote fixed fees for investigations and written reports. You can perform procedures in phases and keep the client informed and involved in the process to avoid surprises.
- *What is the integrity of management?* This question may be assessed periodically during the engagement, particularly if the auditors have relied on any of the individuals during the course of their audit procedures. *Develop an understanding of local management and key personnel.*
- *Are earn-out agreements in effect?* If so, managers may have an incentive to misstate financial results for their own benefit. Understand the payments inuring to local management: housing, credit cards, domestic services (landscaping, cleaning, nanny), ATM withdrawals, tuition for children, vehicle or transportation, security, monthly living allowance.
- *How long have key local managers been in place?* Have any due diligence or public record searches been performed on local management? Does local management have an undisclosed interest in another entity or entities? Some of these issues may be common in developing countries due to a lack of transparency.
- *Are you in a situation in which you are shadowing another team of forensic accounting investigators?* Ensure appropriate communications with all parties, ranging from the special committee to your internal legal counsel. In such situations, consider having initial and ongoing input to the scope of the work plan that the other investigative team is using as the basis for their procedures.
- *What is the timing? When do we start?* The quick answer is usually "yesterday." The practical answer may be "sometime soon," especially if the client wants you to review information and conduct public records searches before you gather additional data and conduct interviews. Deadlines may dictate when you start, when you stop, and to whom you report. Obtain dates of upcoming earnings releases and audit committee meetings; the client may assume that you know these dates and expect you to be there and report the findings to date.
- *Do you have insurance coverage?* Please see the following section, "A Word about Insurance."
- *What is the budget?* Depending on the client, budget restraints may or may not be significant considerations. Consider working in phases to manage budgets and fees. Communication is often key in this area in order to manage the client's expectations in a courteous and open manner.
- *Is outside security warranted? Are there safety concerns?* This is primarily a consideration for global assignments, especially in developing countries and countries undergoing volatile political or social unrest.

- *What else should I know at this time?* This open-ended question may yield pertinent information. A group of forensic accounting investigators poised to launch an investigation once asked this question—and learned that during a prior visit by internal audit, security guards had shot at the auditors' vehicle. Their investigation still went forward, but with the aid of bodyguards.

A WORD ABOUT INSURANCE

Can your client recover fraud losses by making a claim against any insurance policies? To determine the answer to this question, examine these issues with the client's risk manager.

- *Do you have an insurance policy that covers employee dishonesty, errors and omissions, or fidelity claims?*
- *Does the policy have a provision for paying investigative costs?* If so, all or a portion of investigative fees could be covered by the policy.
- *Who is the carrier?* You may already know people at the insurance carrier through prior claims.
- *What is the deductible?*
- *What types of events are covered?*
- *What types of events are excluded? What are the policy limitations, if any?* For example, if the deductible is $100,000 and the policy covers losses up to $500,000, the client may decide not to pursue losses much in excess of the policy limits. The client takes a risk in doing so in that the insurance carrier may not accept some of the transactions claimed as covered losses. By limiting the transaction review, you may lose the ability to substitute other, acceptable claims and also limit the amount of other potential recoveries in addition to the insurance claim—a lawsuit against the perpetrator, for example.
- *To what timeframe does the coverage apply? Months? Years?* If the time period under review is extensive, there may be multiple carriers and claims to consider and prepare.
- *What is the notification requirement after an event has been discovered?* (Example: The policy may require that the insurance company be notified within 30 days of acquiring knowledge of an event.)
- *What is the timing for providing a detailed claim for the insurance company after having knowledge of an event?* You may be able to obtain an extension if you request one, usually in multiples of 30 days. Make the request for extension early in the process to avoid surprises.
- *Is the client required to pursue prosecution to obtain payment under the policy?*
- *Regarding an insurance claim, the forensic accounting investigator can usually assist the client in areas including but not limited to the following:*
  - Identify the pertinent time period for review.
  - Assist in identifying schemes.
  - Quantify and document the impact of the schemes.
  - Conduct background research on companies and individuals that may be parts of the claim.

- Conduct interviews with key personnel to understand the schemes and to identify certain weaknesses in the internal controls that allowed the unauthorized transactions to occur (the insurance carrier will ask about these matters).
- Accompany the client to meet with the insurance company to explain key components of the claim.
- Assist the client in preparing the claim.
- Answer questions of the accounting firm hired by the insurance company to review the client's claim.

EXCEPTIONS AND OTHER CONSIDERATIONS

As previously noted, while financial audits focus largely on materiality thresholds, investigative techniques may well focus on identifying exceptions below the auditor's materiality threshold and also on areas, such as employee morale, which are intangible though observable. For example, the fraud examiner may focus on any of the following.

- Transactions that appear unusual as to:
  - Time (of day, week, month, year, or season)
  - Frequency (too many, too few)
  - Places (too far, too near, unexpected)
  - Amount (too high, too low, too consistent, too alike, too different)
  - Parties or personalities (related parties, oddball personalities, strange or estranged relationships between parties, management performing clerical functions)
  - Results seem too good to be true
- Internal controls that are unenforced or often compromised by higher authorities
- High growth, system changes or updates, or change in personnel that have affected the effectiveness of internal controls
- Employee motivation, morale, and job satisfaction levels that are chronically low
- A corporate culture and reward system that tends to support unethical behavior toward employees, customers, competitors, lenders, or shareholders

Consider the following examples, some of which may not be considered material by financial statement audit standards and others of which look not at recorded amounts but at the circumstances surrounding amounts. Any or all may warrant review in the course of an investigation.

- *Time*. Does it make sense that the transactions under review were recorded on weekends or after hours? This skeptical view can also be applied when reviewing the timing and recording of journal entries as part of an investigation into whether entries are being forced to make the numbers.
- *Frequency*. Does it make sense that Mr. X is paid $4,000 every week? While the individual transactions or total amount may not be material to a financial statement audit, it may be significant that Mr. X works in the mailroom and is receiving large round-dollar payments with little or no documentation.

- *Sequence*. Does it make sense that the invoices from a certain supplier have invoice numbers that are sequential or nearly sequential?
- *Place*. Does it make sense that a company located in El Paso, Texas, supports a charity located in San Diego to the tune of $300,000 per year?
- *Approvals*. Does it make sense that these series of payments are just under the approval threshold? Was that intentional to avoid detection and scrutiny?
- *Location*. Does it make sense that a third-party distributor or sales representative wants to be paid in an offshore account?
- *Amount*. Does it make sense that large round-dollar amounts are paid each quarter with no supporting documentation in the files?
- *Parties*. Does it make sense that one of the highest-paid suppliers has an address that, upon investigation, turns out to be a post office box in a residential suburb?
- *Donations*. Is this donation related to a government official who can influence whether a contract was awarded or retained?
- *Petty cash*. Does it make sense that hundreds of thousands, if not millions, of dollars of transactions were recorded through petty cash? While the financial statement auditor may not blink at petty cash because the account balance on the financial statements is a mere $1,000, the forensic accounting investigator will focus on the activity in the account rather than the balance. The activity can be summarized through the data-mining routines discussed in Chapter 17.
- *Salary levels*. Does it make sense that an office manager for a small subsidiary in rural Illinois makes a salary significantly above the market conditions for that area?
- *Perks*. Does it make sense that the vice president used the company jet to attend a World Series game, when the company had no event sponsorship or business guests to entertain? Probing into salary and perk issues may pinpoint undisclosed payments related to executive compensation. It may also be instructive to see an executive push the limits of rationalization, thereby begging the question, "Where else could he have exercised poor judgment?"

Answers to these types of questions will probably assist the client and forensic accounting investigator in determining next steps. Do everything you can to corroborate verbal responses with related documents. What statements can be substantiated through documents, further inquiry, or third-party sources, including public records searches? The tangible evidence you are looking for includes documents, electronic communications, third-party written confirmations, original bank statements, canceled checks, and the like. Consult with others: Does what you are observing make sense? Probe for the underlying facts.

CONSIDERATIONS ON INTERNATIONAL ASSIGNMENTS

Conducting a global investigation is a complex activity but in many respects rewarding. Your professional skills are likely to be stretched further and exercised more thoroughly than in the past. Those skills include diplomacy. Show appreciation to everyone, from drivers and accounts payable clerks to the managing director. You never know who will call you in your hotel with key information or provide

documents that were allegedly lost, deleted, or stolen—simply because you have treated them courteously and they respect the task you have undertaken.

Performing forensic engagements in foreign places may sound like a dream come true. The dream can become a nightmare, however, without sufficient preparation. As a professional, you are already aware of much that is required, but it is worth remembering that visas and, in some countries, work permits will be required. Pity the poor forensic accounting investigator who is asked to exit a foreign location because of a work permit violation. It may be hard to explain that situation to your client. The rule is to know before you go.

Rather than engaging in comprehensive data gathering, understand the local laws governing privacy, and ensure you are in compliance. As mentioned in Chapter 10, "Building a Case: Gathering and Documenting Evidence," and referenced in Chapter 17, "Data Mining," the most significant and far-reaching example of privacy legislation is the Data Protection Act (DPA) enacted by the European Union. The DPA requires that those who process personal data must comply with DPA principles.

Also, before traveling to underdeveloped countries, consult with a physician to determine whether you should obtain immunizations. Your physician will have access to up-to-date information about required immunizations and matters deserving caution. Ensure that your prescriptions are filled, and consider whether other remedies should travel with you among your personal articles. Some regions in the world are insecure. If personal and team security is needed, arrange for it before your arrival, and never assume that local security resources at a local plant or office are necessarily on your side. On one engagement in a developing country, a local security firm secretly installed listening devices in the conference room where a forensic team was working. For several weeks, local management stayed one step ahead of the forensic accounting investigators, until the light dawned and the forensic team hired its own security.

A global forensic investigation is a remarkable blend of systematic procedure, teamwork on a sometimes vast scale, and individual skill. Courage, perseverance, and intuitive intelligence can make the difference between a successful global investigation and an investigation that loses its way in the complexities of unfamiliar business cultures. Being familiar with simple phrases in the local language can make a positive difference when dealing with local contacts. Also, understand where you are going and what is important in that society. For example, some cultures communicate by e-mail and are more transaction-based. This approach may be ineffective when interacting with relationship-based hierarchical societies. By using some cultural sensitivity, you will achieve better results and can be more confident in your assessment. Also, delays in obtaining information are normal, so prepare yourself for a longer stay than originally scheduled.

There are various considerations to keep in mind when traveling internationally; however, when traveling to emerging markets, keep in mind that systems and infrastructure may present challenges with obtaining information, whether electronic data or from interviews. The level of sophistication varies widely, whether investigating domestically or abroad. One of the keys for success on an international assignment is communication. It is important to rely on local resources with language skills and knowledge of local business practices to obtain optimum results on these types of assignments.

ACCOUNTING ISSUES

When investigating accounting issues, there are some basic items to consider. Confirm that the foreign location's financial statements agree with its local books and records. This point will seem basic; if you are working with a financial reporting package such as Hyperion, however, keep in mind that it may not be a system requirement to interface the general ledger with the reporting package. It is possible to report something different from the local books and records, and in some situations that difference can foreshadow millions of dollars of write-offs or missing funds or both.

Inquire about the local auditor's reputation. Obtain copies of statutory reports and other reports from local auditors. These may include reports to local management, perhaps not sent to corporate, as well as management reports that may not have been communicated to the accounting firm's lead office.

Know where the cash is going. Is the business cash intensive? If the location is a cost center, compare cash requests with cash outflows. Trace cash transfers and the destinations of unknown wires. Review statements for direct payments such as credit cards and ATM withdrawals.

Which are the biggest-paid vendors? Does the pattern make sense? Focus on departmental and noninventory types of payment such as legal, information technology, marketing, promotion, travel, and commissions paid outside parties such as individuals and sales representatives.

Check on travel reimbursements, especially for salespeople. An expense recorded as "gifts" may be given to vendors and customers through this channel as a form of bribe payment. Gifts can range from furniture to electronics such as digital cameras and computers and go even as far as a set of tires. Gifts can also be recorded on credit cards, especially in entities that pay statement balances without much review. Gifts may also appear as marketing expense.

Does the location use a petty cash account? Because petty cash may be a relatively small balance on the financial statements, it may be overlooked by outside auditors and internal auditors alike. The point of interest in petty cash is not the amount on the trial balance but, rather, the amount of activity flowing through the account. Petty cash is a line item through which suspicious transactions can occur with a low probability of detection.

Also, know whether account reconciliations are completed on a timely basis. Obtain and review conciliations for all accounts. If there are large write-offs to key accounts on the balance sheet, consider the following:

- Obtain an understanding of the nature of the adjustment, especially if material.
- Identify the most recent time a 100 percent physical inventory was taken.
- Is inventory stored at offsite locations?
- Are commissions paid at the time of sale rather than the time of bill collection? (The fact here may relate to accounts receivable write-offs as well as revenue schemes.)

Finally, when investigating in a foreign location, it is essential to understand common schemes that occur in that region and sector. This can be accomplished by consulting and using local resources. By failing to make this connection, you

may fail to identify an important scheme. Even sophisticated forensic accounting investigators with years of global experience may overlook this important aspect and cultural sensitivity.

DATA ANALYSIS

Data mining is limited only by your imagination and can be tailored to the data set under analysis. See Chapter 17 for more information on data acquisition and analysis. Some common data-mining queries to identify asset misappropriation may include the following:

- Scanning transactions listings
- Identifying duplicate invoice numbers, payments, or payroll transactions to the same payee
- Analyzing the frequency of payments to vendors
- Sorting payments in descending value
- Summarizing payments by payee to identify where the money is being paid
- Searching for common payment amounts or duplicate amounts
- Identifying gaps, voids, and canceled checks
- Searching for sequential vendor invoice numbers
- Identifying vendors with the same name, different address
- Identifying vendors with the same address and different names
- Filtering to identify all new suppliers, nonstandard journal entries, and accounts under dispute
- Stratifying or grouping customer accounts by balance size or employees by overtime pay

Data-mining analytics are different from the other types of analytic procedures that use aggregated financial information, as they are queries or searches performed within accounts or other client data to identify anomalous individual items. What can be expected of data mining depends on the purpose of the procedure. For example, scanning a numerical sequence may bring to light anomalies that merit investigation, while scanning payment amounts may yield evidence of duplicate payments. The expectation in searching for large and unusual items is based on the forensic accounting investigator's assessment of what constitutes normal. While some analytics such as a scan of closing or adjusting entries may be performed manually, others, such as filters, duplicates, gaps, and sorts, may require computer-assisted audit techniques using software packages or other tools.

DOCUMENT REVIEW

Document review can be critical to a case. Relatively inexperienced people may overlook a feature of a document, while an experienced forensic accounting investigator will view that feature as a potential red flag. Consider the following illustrations.

ComQuest

5837 Karric Square, Suite 130
Dublin, OH 43016

Phone: 801-555-3617
Fax: 801-555-1234

Invoice

Invoice #: 476463
Invoice Date: 03/24/2000
Customer ID: BP-486

RECEIVED BY OPERATIONS DEPT
APR 2 1 2000

Bill to:
ABC Manufacturing
1234 Walnut Drive
Columbus, Ohio

Ship To:
Same as bill to

Date	Your Order #	Our Order #	Sales Rep	FOB	Ship Via	Terms	Tax ID
March 24, 2000		576463	Ken Quinn			Net 30	31-236462

Quantity	Item	Units	Description	Discount %	Taxable	Unit Price	Total
1	PBX-4638	EA	Comdial 6730 Telex Switch	12	N	$17,296.00	$17,296.00
2	ST-786T	EA	Comdial 6810 CSU/DSU	10	N	$3,625.00	$3,625.00
76	LBR-06	HR	Labor	0	N	$85.00	$6,460.00
						Subtotal	$27,321.00
						Tax	
						Shipping	
						Other Charges	
						Total Due	$27,321.00

REMITTANCE

Customer ID: BP-486
Date: **03/24/2000**
Amount Due: **$27,321.00**
Amount Enclosed: _____

Communications for the next millennium

EXHIBIT 14.1 ComQuest Invoice

ComQuest

Exhibit 14.1 reproduces an invoice from what proved, through investigation, to be a phony company. This invoice was approved, submitted for payment, and subsequently paid. While the document deceived the accounts payable clerk and the check signer, close examination reveals a series of red flags.

Invoices typically have an address, telephone number, contact name, reference number, and description of parts and services along with amounts, taxes, and so

forth. While this invoice does show an Ohio address, the 801 area code is in Utah! Note the icon on the right—a woman speaking on the telephone. In style, it is straight from the 1950s. Compare this icon with the tagline at bottom right: "Communications for the next millennium." The icon is probably so-called clip art downloaded from a cost-free online image bank.

Note the invoice's columns for Quantity, Unit Price, and Total. We would expect these numeric amounts to be right justified with decimal points aligned, not left justified. Focus on the second line item, indicating that two items, identified as Comdial 6810 CSU/DSU, were purchased. The unit price is the same as the total. If this were produced on a bona fide electronic invoicing system rather than with a word processing program, one would expect the system to calculate correctly.

Here is a finer point: The tax ID number (see right column in the middle of the document) is an eight-digit number. It should be a nine-digit number. Also, while there is an address on the invoice, it was easily proved to be a mailbox drop business. Last, the invoice had no folds, strongly suggesting that it was produced in-house and not actually mailed as would be expected from a valid vendor.

CPA Services

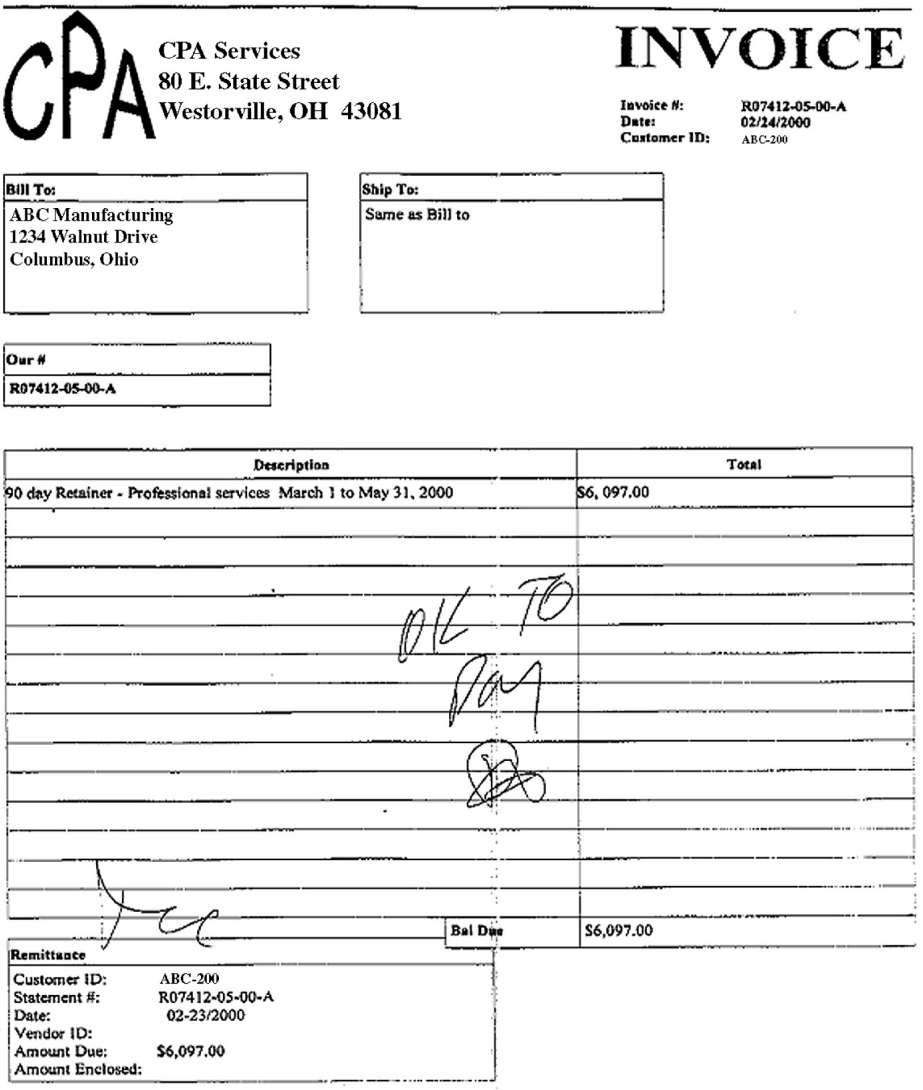
The second invoice, Exhibit 14.2, appears to be for CPA services. Note that there is no telephone number, fax number, or contact name. The invoice is allegedly a retainer for professional services, but not the round-number amount you would normally expect to see. A directory investigation would in time show that *CPA Services* is actually an acronym for *Columbus Preferred Apartments*. An inquiry with that entity would then show that the payment was for an apartment rental rather than professional services.

Note there is a *Ship to* section on the invoice. One would not expect *Ship to* on an invoice for professional services (or, for that matter, for rent on an apartment). The dates in the upper right and lower left are different from each other and in inconsistent formats. The invoice amount is left-justified. Finally, be mindful of generic vendor names as potential red flags.

How to Read a Check

Exhibit 14.3 illustrates the information found on a typical check. Forensic accounting investigators with knowledge of the codes for the Federal Reserve districts, offices, state, and bank identification numbers may be able to easily identify a forgery. Additionally, another key number on the check is the magnetic ink character recognition (MICR). The MICR includes the paying bank's ABA (American Banking Association) routing number, the account number of the writer of the check, and usually the sequential check number. If the check number in the MICR does not match the check number at the top of the check, that may be an indication of a forged check.

The endorsement of the payee is located on the back of the check. Other important information found on the back of the check is the date and name of the bank where the check was deposited and the date and location of the Federal Reserve office through which it was routed. By following the endorsements, a forensic accounting investigator can follow the path from the point at which a check was deposited to



CPA Services
80 E. State Street
Westorville, OH 43081

INVOICE

Invoice #: R07412-05-00-A
Date: 02/24/2000
Customer ID: ABC-200

Bill To:
ABC Manufacturing
1234 Walnut Drive
Columbus, Ohio

Ship To:
Same as Bill to

Our #
R07412-05-00-A

Description	Total
90 day Retainer - Professional services March 1 to May 31, 2000	$6, 097.00
Bal Due	$6,097.00

OK TO PAY

Remittance
Customer ID: ABC-200
Statement #: R07412-05-00-A
Date: 02-23/2000
Vendor ID:
Amount Due: $6,097.00
Amount Enclosed:

EXHIBIT 14.2 Invoice for CPA Services

the point at which it was cleared. When reviewing checks that are hand signed rather than electronically signed, a forensic accounting investigator should compare the signature on the front of the check with the signed endorsement and look for similarities. Although forensic accounting investigators are not necessarily handwriting experts, they should be able to notice whether or not certain letters look similar.[3]

[3] Jack C. Robertson, *Fraud Examination for Managers and Auditors* (Austin, TX: Viesca Books, updated annually).

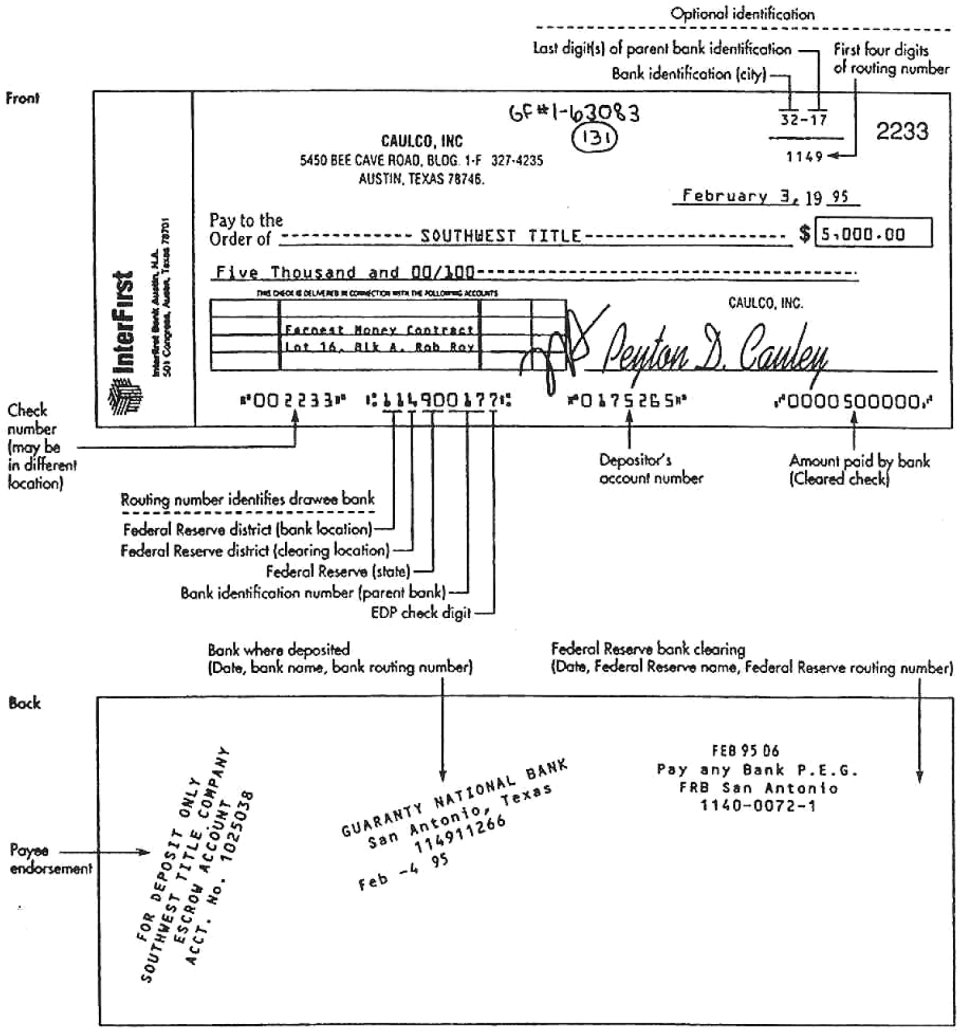


EXHIBIT 14.3 How to Read a Check

Airline Tickets

While we have not included an airline ticket exhibit, some basic information on this topic may be helpful for expense report reviews. Many tickets issued as e-tickets with an e-ticket itinerary and receipt may contain sparse information. However, these documents may still contain the passenger's name, travel destinations, ticket price, travel dates, and class. An important aspect of a paper or e-ticket is the form of payment. Usually, the credit card number is masked, with the exception of the last four digits, for security purposes. The last four digits can be matched to an employee's credit card number to trace the payment to the passenger.

Another fraud that forensic accounting investigators should look for is duplicate payment. Duplicate payments (collusion) can occur when another person charges the

ticket and the passenger then submits the ticket for reimbursement as well. Duplicate payment can also occur if an itinerary is accepted as proper documentation for reimbursement. Companies should refrain from accepting itineraries as acceptable documentation, since an itinerary can be obtained and then canceled without the employee actually making the trip.

Obtaining details of expense reimbursements in an electronic file can assist in identifying duplicate payments. With some basic sorting and analysis, transactions may come to your attention that could be missed if total reliance is placed on sampling or hard-copy review.

CONCLUSION

This chapter has provided a taste of what a forensic accounting investigation is like and how it differs from a financial statement audit. Although the educational backgrounds of the financial auditor and the forensic accounting investigator may be similar, the mind-set and work processes are drastically different. No two investigations are alike, and "last year's workpapers" do not exist in these situations. Further, materiality has little meaning to the forensic accounting investigator.

We have also illustrated various reasons why an investigation can become necessary and the considerations that must be weighed by the forensic accounting investigator in planning the investigative approach. The next chapters will guide you through the investigative process even further and explore in greater detail many of the investigative techniques mentioned in this chapter. Applied effectively, these techniques can crack the case—although the usual caveat applies: There will usually be some degree of corporate fraud, and some portion of it cannot help but go undetected or unresolved.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 15

Corporate Intelligence

David Jansen, Glenn Ware, and Alexander Kapur

As forensic accounting has become an essential tool to investigate fraud, corruption, and other forms of financial misconduct, the related, but distinct instrument of corporate intelligence has evolved to play a similar role. As opposed to relying on targeted review and analysis of the numbers in a company's financial statements, books, and records to identify high-risk or otherwise unusual transactions, the practice of corporate intelligence centers on research and analysis of qualitative information regarding a subject of interest, being either an entity, a person, or an issue.

Corporate intelligence and forensic accounting teams often work in tandem to identify and mitigate potential or current risks facing an organization, and help resolve questions arising from quantitative abnormalities.

DEFINITION OF CORPORATE INTELLIGENCE

Corporate intelligence is broadly defined as the focused collection and analysis of information regarding an unfamiliar subject that is used to deliver key insights to decision makers in support of a major business concern, corporate action such as an investment or acquisition, internal inquiry, or consideration of risk factors. This information is largely obtained through public records, open sources, and proprietary databases. It can also be developed through interviews and conversations with knowledgeable individuals. When access permits, such as in the case of a friendly merger or acquisition, these independent sources of information can be further supplemented by an overt, detailed review of a target's internal business information, providing the most powerful and accurate outcome.

A corporate intelligence product is highly customizable, depending on the nature of the inquiry, the required level of detail, and its consumer. Its ultimate form generally depends on the context in which it is deployed and the type of subject of interest. Corporate intelligence that serves to support overall pretransaction due diligence on a potential acquisition target, for example, is quite different from that used to evaluate the types of operational risk that might arise from a company's decision to conduct business in a high-risk country or outsource a business process to a remote location. Therefore, to say that the definition is fluid is correct.

Corporate intelligence can also be defined by its distinction from closely related disciplines. Similar terms, such as *business intelligence, competitive intelligence,* and *strategic intelligence,* are often misapplied, intermingled, and otherwise incorrectly used with *corporate intelligence*. This confusion is mostly attributed to the relative immaturity of these practices compared to other traditional organizational functions, such as treasury, human resources, and marketing, but is also a result of the natural synergies between these disciplines.

- *Business Intelligence:* It has been more recently defined as a corporation's structured handling and manipulation of data gathered during the normal course of business to help guide the company's strategic decisions. Its definition has an inward-facing connotation and frequently involves exploitation of data-mining tools, artificial intelligence, knowledge management, and information technology. The intended outcome is to improve a company's responsiveness to certain environmental stimuli, such as a shift in consumer preferences. A good example of a business intelligence practice is a refined approach to customer data management such as using incentive programs through memberships to gather data about consumers while they make their purchases.
- *Competitive Intelligence:* It's a form of corporate intelligence, but it focuses narrowly on competition, and is meant mostly to drive commercial marketing and strategy by enabling companies to position themselves apart from and ahead of the competition. Through careful study of a competitor's planning, strategy, marketing tactics, and profitability, a company can anticipate and prepare for a competitor's actions.
- *Strategic Intelligence:* This is the thoughtful integration of all of an organization's intelligence streams, including corporate intelligence. Jay Liebowitz, the author of a recent book titled *Strategic Intelligence,* writes, "In the business setting, SI has a similar meaning as that under military intelligence vogue, but the emphasis is on how best to position the organization to deal with future challenges and opportunities to maximize the firm's success."[1] Strategic intelligence, therefore, is a holistic and comprehensive combination of all forms of organizational intelligence.

EVOLUTION OF CORPORATE INTELLIGENCE

Although the term *corporate intelligence* is a relatively fresh term in the vocabulary of today's international trade and commerce, it is not an entirely new phenomenon. The ways in which the tool is applied have evolved greatly, however. Four hundred years ago it was first used as a way to navigate to desired trading posts, whereas it is now used to detect and mitigate the spectrum of business risks, including fraud and corruption.

The need to know and understand one's operating environment, potential business partners, and the risk of transactions is as old as international trade

[1] Jay Liebowitz, *Strategic Intelligence: Business Intelligence, Competitive Intelligence, Knowledge Management* (Boca Raton, FL: Auerbach Publications, 2006).

itself. Scott Moeller, a published authority on intelligence used for merger and acquisition (M&A) purposes, demonstrates this point well by citing early forms of commerce-driven gathering and synthesis of information to facilitate business interests:

> *In the late 16th and early 17th centur[ies], commercial intelligence was considered essential for East India Company's trading. Richard Hakluyt was appointed in 1602, for example, "to set down in writing a note of principal places in the East Indies where trade is to be had." Hakluyt had already published* The Principal Navigations, Voyages, and Discoveries of the English Nation, *a tome which* [sic] *consisted of over 500 reports collated from the complete gamut of European travelers, including explorers to pirates to colonists. These reports provided data on navigation, geography, resources, politics, and economics from every corner of the known world.*[2]

From information that was used to help traders navigate the globe and understand completely exotic territories and people, the focus on this intelligence gathering remit shifted as the world became smaller and competition increased. Companies that had traditionally been sole providers in their field witnessed the emergence of numerous domestic and foreign competitors who threatened their market dominance. The growth of state-owned companies in regimes from the Far East and Communist bloc countries also infused the use of defense and military intelligence mechanisms to challenge their free market counterparts, mostly Western European and American. Thus, commercial intelligence emerged to become one of the tools leveraged to attack the competition, and corporate espionage became a known factor in business operations. Hedieh Nasheri, author of a recent book on corporate espionage, states:

> *Espionage is the collection, collation, and analysis of illicitly gained information. In the case of industrial espionage, the most common objectives are to determine competitor activities with regard to new products, formulations, research areas of interest, production methodology, production quantities, promotional programs, distribution, and economics, pricing, etc. . . . to time markets and establish pricing.*[3]

Two forces shifted the orientation of corporate intelligence or espionage from an entirely offensive tool used for nefarious purposes to an equally defensive countermeasure and institutionalized system: the realized losses suffered by companies as a result of corporate espionage, and the change in the frequency and nature of mergers and acquisitions.

---

[2] Scott Moeller and Chris Brady, *Intelligent M&A: Navigating the Mergers and Acquisitions Minefield* (West Sussex, UK: John Wiley & Sons, 2007).
[3] Hedieh Nasheri, *Economic Espionage and Industrial Spying* (Cambridge: Cambridge University Press, 2005).

As corporate espionage gained popularity as a way to undermine competition and even attack entire economies, the defense mechanisms against espionage became more sophisticated. In 1983, U.S.-based Motorola CEO Robert W. Galvin, who had served on President Reagan's Foreign Intelligence Advisory Board, hired Jan Herring, a veteran from the CIA, to develop the first "corporate intelligence" division in the United States's private sector.[4] Galvin established this practice as a countermeasure to the costly theft of Motorola's trade secrets and technology production methodologies. Galvin feared that foreign intelligence agencies, not only from Soviet bloc and China, but also France, Israel, and Japan, were stealing Motorola's trade secrets to provide them to rivals abroad.[5] The immediate purpose of the internal corporate intelligence unit was to identify high-risk entities and individuals with which Motorola was doing business so as to identify the company's vulnerabilities to these unknown quantities and reduce the looming threat of security breaches by them. This intelligence deployment was the first time that such a formalized division would be used for defensive purposes in commerce.

In addition to corporate espionage, the sharp uptick in 1980s mergers and acquisitions also created a need for formalized corporate intelligence practices. The relaxed antitrust enforcement under the Reagan and Thatcher administrations in the United States and United Kingdom brought about a fierce merger wave that spanned from 1981 to 1989. The popularity of mergers and acquisitions grew in numbers as a way for companies to grow, expand market share, and eliminate the competition. Hostile deals and takeovers matured as a method to acquire desired business targets. Corporate raiding developed as a method to secure key assets. With these new methods, corporate intelligence became a necessary tool for two purposes: to support a client engaged in fierce proxy battles by undermining adversarial management through negative information campaigns, and to ensure that target businesses could be integrated into the acquirer's existing structure.

The rapid globalization of business in the 1990s and 2000s also contributed to the rise of today's use of corporate intelligence. The opportunities presented by new, high-growth overseas markets provided companies with a new way to expand. An emphasis on efficiency allowed businesses to become more specialized and to outsource business processes to overseas providers that enjoyed lower operating costs. Relaxed international trading provided businesses with a new way to source raw materials, cheaper labor, and other key supplies from foreign territories. However, with this globalization, the risk of international operations also grew, so company executives were forced to learn more about unique threats presented by the unknown market suppliers, vendors, and customers. Corporate intelligence is now key to fostering a greater understanding of the risks lurking in the lesser-known corners of the world.

Corporate intelligence products today are highly sophisticated, providing business leaders with information they need to operate on a global scale with workforces, partners, and customers in foreign lands. Beyond mere background checks, corporate intelligence has grown to become an essential risk mitigation tool.

---

[4] www.scip.org (Society for Competitive Intelligence Professionals).
[5] Adam L. Penenberg and Marc Barry, *Spooked: Espionage in Corporate America* (New York: HarperCollins, 2000).

TODAY'S BUSINESS NEED

Strategic business M&A, legal, compliance, and marketing efforts all require corporate intelligence support. The benefits of the modern global marketplace prove to be fruitful to most businesses as long as the heightened risks are identified, contemplated, and appropriately managed. Corporate intelligence fosters a far deeper understanding of the various risks posed by legal, regulatory, brand and reputation, physical, political, financial, personnel, intellectual property, information technology, competitive, and contractual or transaction domains.

In his book *Corporate Radar,* Karl Albrecht, an expert on corporate risk management, alluded to the many business aspects that should be contemplated when conducting corporate intelligence. Regarding management of anticipated risks, Albrecht said, "An executive team should not be frightened into immobility by the unlimited number of possible threats that could arise, but a thorough business scan must include these kinds of possibilities in addition to the more commonplace issues.[6] He continued, "Every corporation needs figurative radar. Your corporate radar is the disciplined process of investigating, studying, analyzing and thinking about the various dimensions of your business environment."[7] Corporate intelligence is a main component of that continuous radar sweep.

LEGAL AND REGULATORY DRIVERS OF CORPORATE INTELLIGENCE

The current legal and regulatory frameworks governing international commerce are far more complex and punitive than those existing even 20 years ago. International and multilateral organizations and governments of the developed world have constructed a series of new laws and rules and increased enforcement of existing ones, the purpose of which is to level the playing field of international business, to reduce corruption to eliminate criminal access to business and legitimate financial systems, and to curb other forms of misconduct and injustices to which the commercial sector is susceptible. Burgeoning anticorruption and transparency legislation, refined labor and employment laws, intellectual property rights, know your customer (KYC) provisions, banking and investment restrictions, environmental and human rights safeguards, and stringent export controls are just a few examples of the increasingly complex nature of the legal and regulatory environment facing business organizations.

Coinciding with stricter legislative and regulatory environments, regulatory agencies have placed greater and greater expectations on private enterprise to monitor and enforce regulations on their own operations. This self-policing arrangement "assigns to [the] private sector the bulk of the responsibility for enforcement, which they undertake by implementing agreed management practices that are taken to show

[6] Albrecht, 5.
[7] Albrecht, 7.

'due diligence.'"[8] The following are a sampling of the major legal and regulatory drivers that call for and define such due diligence, which can be achieved through appropriate deployment of corporate intelligence.

Federal Sentencing Guidelines: Due Diligence and Vicarious Liability

Management's ignorance of risks associated with doing business in certain regions or with certain entities or individuals is no longer always a defensible position to respond to allegations of corporate malfeasance or other misconduct. Case precedents demonstrate that the U.S. judicial system places the responsibility for organizational behavior with top management (Dow and Muehl 1992; Fargason 1993). Corporate governance standards require increasing accountability and transparency of boards, which have been forced to be more involved in risk management practices and to bear more responsibility in the wake of an incident. "Senior executives are also facing more detailed questioning about their strategy and decisions."[9]

This relatively recent shift in the burden of responsibility for corporate conduct is highlighted by the 2004 U.S. Sentencing Guidelines, as amended.[10] The guidelines allude to the concepts of vicarious liability and due diligence as key factors in sentencing corporations and individuals for misconduct perpetrated by an organization or by individual employees in the course or scope of employment. Until recently, individuals have been historically protected by various liability provisions, but the principle of vicarious liability signifies how individuals and the corporate entity itself can be held liable if the organization or its employees or agents have not followed the minimum requirements of the federal sentencing guidelines.[11]

Given the greater onus on management to ensure good corporate behavior, the significance of ensuring that a company conducts due diligence using, in some cases, corporate intelligence capability, could not be more important.

Section 8B2.1 of the November 2004 U.S. Sentencing Guidelines states that an "effective program to prevent and detect violations of law" means a program that has been "reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct, . . . the organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual [who] the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program."

---

[8] Kathryn Gordon and Maiko Miyake, "Approaches to Combating Bribery: A Study of Codes of Conduct," *Journal of Business Ethics* 34(3) (2001): 161–173.
[9] Moeller, 73.
[10] Sentencing policies and practices developed by the U.S. Federal Sentencing Commission for the federal criminal justice system that will assure the ends of justice by promulgating detailed guidelines prescribing the appropriate sentences for offenders convicted of federal crimes.
[11] Norman O. Schultz, Allison B. Collins, and Michael McCulloch, "The Ethics of Business Intelligence," *Journal of Business Ethics* 13(4): 309–311.

The concept of *due diligence* is specified in seven broadly interpreted steps,[12] summarized here:

1. Compliance standards and procedures applicable to employees and agents
2. High level oversight and maintenance of that compliance function
3. Due care not to delegate authority to individuals known through exercise of due diligence to have propensity to engage in illegal acts or unethical behavior
4. Effective communication of standards and procedures to employees and agents
5. Compliance with standards through monitoring, auditing, and reporting systems reasonably designed to detect criminal conduct by employees and other agents
6. Consistent enforcement through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense
7. Reasonable response to act appropriately to the offense and to prevent further similar offenses

Corporate intelligence is an instrument that organizations can use to aid in meeting required minimum standards of detection and monitoring for due diligence purposes.

Anticorruption and Counterfraud Laws and Regulations

The last ten years have witnessed marked development of anticorruption, counterfraud, and transparency laws and regulations. This momentum has occurred at all levels of government, from the signing of conventions by member countries to international organizations, to legislative reforms at the country level, to state law initiatives. Significantly, this trend is in response to calls for institutions in developed nations to remove high-toned rhetoric and act instead to enforce their existing treaty obligations and embed anticorruption practices in international financial agencies.[13] Many laws and expert opinions cite due diligence as a critical component of effective compliance with these legal and regulatory obligations.

The following is a partial list of major conventions, rules, laws, regulations, and governing bodies that cite due diligence as an effective and necessary measure to prevent corruption and fraud.

United Nations Convention Against Corruption

Organisation for Economic Co-operation and Development (OECD) Convention on Combating Bribery of Foreign Officials in International Business Transactions

World Bank

International Chamber of Commerce

---

[12] Robert J. Rafalko, "Remaking the Corporation: The 1991 U.S. Federal Sentencing Guidelines," *Journal of Business Ethics* 13(8): 628–629.

[13] Ben W. Heineman Jr. and Fritz Heineman, "The Long War Against Corruption," *Foreign Affairs,* May/June 2006.

Financial Investigations Bureau (FIB)

U.S. Foreign Corrupt Practices Act

Transparency International's Business Principles for Countering Bribery

The World Economic Forum's Partnering Against Corruption Initiative (PACI), Principles for Countering Bribery

Especially in the United States, the increased rate of enforcement of the Foreign Corrupt Practices Act (FCPA) has elevated the need for organizations to perform due diligence on foreign business partners, agents, vendors, and customers in an effort to prevent and detect bribery or other illicit influence of foreign government officials and political figures. Federal prosecutors are pursuing significant fines and prison time for executives who fail to conduct adequate due diligence or willfully ignore bribery risks.

A law firm specializing in FCPA prosecution defense recently noted a release regarding Department of Justice and SEC enforcement trends in 2009. The release opened:

> *2009 was one of continued heightened FCPA enforcement activity. It is a year that will be remembered for more records and "firsts": A year that started with imposition of the second-highest FCPA-related penalty (US$579 million) in the KBR/Halliburton case and the highest penalty to date for a U.S. company; a year when new prosecutorial tools were unleashed in FCPA cases, such as control person liability; a year when foreign officials became targets for prosecution; a year when a focus on individual prosecutions clearly emerged; and a year that ended with a flurry of activity, which has continued into 2010.*

The release concluded, "Both the DOJ and SEC have requested budget increases for the upcoming fiscal year that would give them additional resources to substantially increase their FCPA enforcement activity. . . . The FCPA Unit is expected to develop industry-wide investigations and regional expertise."

And though the U.S.-based FCPA is one of the greatest drivers of corporate intelligence, international conventions and overseas legislation are enhancing their provisions for corporate minimal ethical and "good conduct" standards, oftentimes to include due diligence procedures. In March 2010, the OECD released new practice guidelines, defining "Good practice guidance on internal controls, ethics, and compliance." Within those guidelines, the OECD explicitly states that "properly documented risk-based due diligence pertaining to the hiring, as well as the appropriate and regular oversight of business partners" is an essential element of good practice guidance for companies.

In July 2009, the U.K. Serious Fraud Office (SFO), the law enforcement agency that investigates and prosecutes fraud and corruption, outlined key elements of corporate compliance programs that the enforcement body would assess to determine whether or not to prosecute a company criminally or civilly if an employee was found to have breached anticorruption laws. According to a March 2010 article released by *Bloomberg Law Reports,* "Under the current version of the SFO's Guidance for Investigating Draft Bill, a company may be held criminally liable if one of its

employees is found to have committed bribery unless the company can establish it had adequate procedures in place to prevent bribery. While the Draft Bill does not explain what will constitute *adequate procedures,* the SFO Guidance suggests that a company's anti-bribery procedures should resemble in large part the seven elements of an effective compliance program set forth in the U.S. Sentencing Guidelines." Specifically, the SFO stated that it would consider whether the corporation exercised "diligence and appropriate risk assessments," and conducted "regular checks and auditing in an appropriate manner."

Anti–Money Laundering and Financial and White Collar Crime Legislation

Closely related to the surge in anticorruption and transparency initiatives is the concentrated effort to prevent and prosecute money laundering and other financial crimes that benefit organized crime and terrorists. This ambition is a product of the obvious need to restrict criminal access to and use of the global financial system.

As with anticorruption and transparency, there are several international conventions, law enforcement agencies, prosecuting authorities, laws, regulations, and rules that identify due diligence as a necessary practice to combat money laundering and financial crime. These include, but are not limited to:

- OECD Third Directive on Money Laundering
  - United Nations Treaty on Organized Crime
  - Basel Committee on Bank Supervision, Customer Due Diligence Principles
- Financial Action Task Force[14] Recommendation 7
  - Financial Crimes Enforcement Network (FINCEN) Rules XXX Corresponding to Enhanced Due Diligence of Foreign Correspondent Bank Accounts
  - U.S. Patriot Act
  - U.S. Bank Secrecy Act

As specifically outlined in these legal and regulatory frameworks, companies that seek to comply with these laws and regulations are required to implement risk-based, enhanced due diligence programs.

COST DRIVERS OF CORPORATE INTELLIGENCE

While corporate intelligence and due diligence are investments that must be contemplated in organizational expansion and development budgets, the cost is recovered

[14] The Financial Action Task Force (FATF) is an intergovernmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a policy-making body that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published Forty Recommendations on Money Laundering and Nine Special Recommendations on Terroist Financing to help meet this objective.

not only by savings of reduced penalties if something goes wrong but also by mitigating the costs of a bad corporate action.

Reduced Monetary Penalties

Recent case outcomes prove that companies with tough ethics policies, inclusive of rigorous monitoring and due diligence systems, may receive more lenient treatment if they cooperate with prosecutors and their policies meet the legal standards. For example, a fine of $1 million to $2 million could be knocked down to as low as $50,000 for a company with a comprehensive program.[15] Judge William W. Wilkins Jr., then-chairman of the U.S. Sentencing Commission, was quoted in an article concerning business ethics, stating that: "Even the best efforts to prevent crime may not be successful in every case. But we have to reward the corporation that was trying to be a good corporate citizen."[16]

Cost of Failed Corporate Actions and Strategic Relationships

Though the estimates surrounding failure rates of M&A integrations vary, they tend to range between 40 and 70 percent. One source stated, "Most [mergers] fail to add shareholder value; indeed, post-merger, two thirds of the newly formed companies perform well below industry average."[17] Victor Cook, a professor of marketing and strategy at Tulane University, estimated the magnitude of lost dollars in airline mergers alone. "Since deregulation in 1978, traditional, full-service airlines, also known as 'legacy' carriers, have lost a combined US$29.6 billion on ill-conceived mergers."[18]

To mitigate this rate of failure and reduce the associated costs, companies are urged to conduct thorough financial, regulatory, and even cultural evaluations before their mergers and acquisitions. Mark Baxter, a strategic business advisor, commented on the importance of due diligence, especially for cultural aspects, surrounding mergers and acquisitions. He writes:

> *The technique of assessing a business through analysis of its functionality can form the basis of a cultural due diligence practice, which assesses specifically the level of match between two organizations by exploring the areas of alignment (or lack of). By using these assessments alongside the commercial due diligence procedures, the likelihood of failure is mitigated and the potential to reach financial and operational goals increased.*[19]

---

[15] Bruce Hager, "What's Behind Business' Sudden Fervor for Ethics," *Business Week,* September 23, 1991.
[16] Robert J. Rafalko, "Remaking the Corporation: The 1991 U.S. Federal Sentencing Guidelines," *Journal of Business Ethics* 13(8): 628–629.
[17] Harvard Management Update 2009.
[18] Victor J. Cook, Jr., "Why Airline Mergers Don't Work," *Strategy + Business,* June 2008.
[19] Mark Baxter, "Risk Is for Everyone, Not Just Management," *The Lawyer,* February 5, 2007.

NEGOTIATION DRIVERS OF CORPORATE INTELLIGENCE

Corporate intelligence is not only important to achieving compliance with laws and regulations, and managing certain costs of strategic decisions, but is also used to uncover key points of leverage for improving positioning in contractual negotiations and proxy battles.

In discussing the utility of such intelligence-gathering processes before a merger, Tom Taulli, author of *The Complete Guide to M&A,* states, "You should use any flaws the [due diligence] audit uncovers to negotiate down the sales price." Due diligence, therefore, is "a chance to get a better deal."[20] Deal flaws can include anything from unstable debt positions that were previously undisclosed, to looming legal judgments, or reputational concerns, such as ongoing criticism from NGO groups, all of which can negatively affect the value of a company.

In using corporate intelligence as a defense mechanism to fend off unwanted acquirers, courts support boards in rejecting offers if they can demonstrate negative findings secured from a due diligence process on the acquirer. Companies regularly use corporate intelligence against their adversaries in the court of public opinion.[21]

Triggers

The environmental and situational catalysts of deploying corporate intelligence are many. They depend on the structure and size of the organization, the industry in which it operates, the nature of its business operations, the rigor of regulation, visibility and media scrutiny, the customer base, and its global footprint, just to name a few.

The theater of operation is one of the biggest factors influencing the use of corporate intelligence. Companies with operations in the developing world that are less regulated and transparent are exposed to myriad risks. Albrecht, the author of *Corporate Radar,* notes, ". . . in legally immature societies, you may face a range of legal handicaps, including theft, sabotage, extortion, and terrorism, as well as . . . fraud, violation of contracts, and theft of intellectual property."[22] Regarding the high potential for corruption in these territories, he writes, ". . . the difference between a bribe and a 'commission' paid to a commercial go-between in a Third World country is often a matter of interpretation. Small monarchies, for example, seem to . . . abound with business agents, brokers, and consultants, all of whom seem to trace their bloodlines to a king, shah, emir, or sultan, or other grand poobah. Red tape disappears and approval cycles suddenly accelerate after they receive their respective payments."[23] A number of global standardized risk indicators, such as Transparency International's (TI) Corruption Perceptions Index, help to determine the need for corporate intelligence.

A company's business structure and development strategy is another significant consideration in the use of corporate intelligence mechanisms. Companies that are

---

[20] Darren Dahl, "How to Conduct Due Diligence," *Inc.* 26(10): October 1, 2004.
[21] Moeller, 136.
[22] Albrecht, 220.
[23] Albrecht, 222.

frequently engaged in mergers and acquisitions rely on joint venture partnerships, especially with state-owned companies; maintain a highly autonomous workforce or contracted workforce, such as sales agents; have outsourced or offshore business processes; maintain complex logistics and supply chains; or conduct significant business with related parties that are vulnerable to fraud and malfeasance.

Other situations in which corporate intelligence may be deployed include:

- The presence of complex business structures, such as layered holding companies
- Involvement of state-owned enterprises in the business
- Jurisdictions in which political and commercial sectors are intertwined
- Companies dealing with highly controlled raw materials, products, or state-owned natural resources
- Unknown or otherwise unfamiliar origins of funds from potential investors
- Ventures involving or dependent on major infrastructure, especially in developing nations
- Business in industry sectors well known for fraud and corruption, such as construction, extractive industries, and defense

Both public and private sector entities have also used corporate intelligence in support of:

- Legal strategy to secure key evidence or to anticipate the maneuvers and arguments of their adversaries
- Market entry to map key players and stakeholders, identify landscape risks, and so forth
- Bankruptcy petitions and adverse proceedings to identify hidden, undisclosed, or otherwise absconded assets
- Ability to pay and credit risk assessments to evaluate a prospective debtor
- Asset searches in litigation or arbitration proceedings and settlement calculations
- Export controls compliance
- Supply chain protection and integrity
- Intellectual property security

BASIC DEPLOYMENT AND CONSUMPTION OF CORPORATE INTELLIGENCE

Approaches to corporate intelligence are fluid, dictated by the ultimate user's concerns, questions, and goals. Methodology is influenced in part by the type of industry on which an inquiry is centered; where the intelligence-gathering function is based and from what jurisdiction the intelligence is being gathered; overt versus a discreet inquiry; availability of public information; the level of detail necessary to complete an inquiry; and the existence of conflicts and contrary information in the remit.

The basic framework for corporate intelligence is borrowed from military and government intelligence communities, adapted to the legal parameters of civilian business activities and to orient it for collection of data to be used for commercial purposes. The common elements of the intelligence-gathering process are as follows:

The intelligence remit is devised by decision makers.

Researchers use available information to conduct appropriate public, overt, and discreet inquiries.

Relevant findings from various sources are analyzed in context and delivered to decision makers.

Any further intelligence remit is modified and redeployed depending on findings and analysis of existing remit.

The pool of informative sources from which intelligence is drawn is also fairly stable, but can be scaled according to the jurisdictions of interest, the type of information sought, and the level of detail needed to fulfill the remit. These include, but are not limited to:

- *In cases of consensual due diligence:* self-reported background information (resume or CV or corporate profile); questionnaire responses; books and records; material contracts
- *Electronic sources:* open source (Internet) information; public access online registries, databases, and information repositories; syndicated and proprietary databases
- *Hard-copy public records:* court filings, archived newspaper and periodical information, shareholding certificates, property records, other certified or notarized documents
- *Knowledgeable human sources:* subject-matter and industry experts; current and former business associates and affiliates; litigation adversaries; creditors; customers and clients; competitors; regulators; current and former shareholders or investors; current and former law enforcement and intelligence officers

Background Information and Questionnaire Process

In cases of consensual due diligence, background entity or individual information such as corporate registration documents or education degrees may be provided voluntarily by the subject. Furthermore, the party conducting due diligence may request that the subject entity or individual or both complete a detailed questionnaire. A questionnaire is typically constructed with two main purposes: to secure those basic fields of information necessary for conducting research, such as personal and corporate identifiers, and to survey specific areas of relevant risk posed by the subject, such as potential connections to government entities and officials, criminal history, or ongoing litigation.

Care must be taken to ensure that the questionnaire adheres to legal restrictions governing solicitation and handling of sensitive information, especially those questionnaires pertaining to individuals. Certain jurisdictions, such as those in the European Union, have strict regulations that govern requests for personal information and the transfer of that information to overseas territories, even for due diligence purposes.

Depending on how detailed and invasive the questionnaire is allowed to be, this instrument can secure data that are parallel to the fields explored by the independent research and analysis process.

Once the information has been secured, the information provided can be used to facilitate aspects of the research process. Furthermore, the corporate intelligence team cross-analyzes data provided in the questionnaire with findings from independent research to identify discrepancies, misrepresentations, and material omissions.

CUSTOMARY DATA FIELDS NECESSARY TO FULFILL CORPORATE INTELLIGENCE REMITS

As previously stated, corporate intelligence gathering is defined partially by the answers sought, and therefore, the elements of data collection change accordingly.

When deployed for due diligence purposes, the typical components of intelligence products most frequently include the following elements as they pertain to entities or individuals.

Individuals

- Confirmation of identity or highlights of conflicting information or multiple identities
- Professional history
- Shareholding interests
- Corporate affiliations and board membership
- Education credentials, certifications, and licenses
- Criminal records and litigation
- Civil litigation and bankruptcy petitions
- Regulatory or disciplinary actions
- Liens, judgments, tax warrants, and Uniform Commercial Code (UCC) filings
- Creditworthiness and history
- Media coverage
- Human source feedback

Entities

- Confirmation of corporate identifiers and registration information
- Jurisdiction of business
- Corporate background
- Corporate structure, shareholding, and affiliated businesses
- Major shareholders
- Key management
- Board of directors
- Jurisdiction or location of business
- Certifications, licenses, operating permits
- Criminal litigation
- Civil litigation and bankruptcy petitions
- Regulatory or disciplinary actions
- Liens, judgments, tax warrants, and UCC filings
- Creditworthiness and history
- Media coverage
- Human source feedback

Despite these staple components that guide intelligence gathering, the need for creativity in an approach to corporate intelligence is just as important for meeting information objectives tailored for a specific inquiry.

ANALYSIS AND REPORTING OF FINDINGS

While effective research is essential to formulating a strong foundation of data, the most critical processes of the corporate intelligence function are analysis and reporting.

When the research is complete, corporate intelligence professionals filter resultant findings to isolate the most salient research outcomes. The ensuing analysis process connects seemingly disparate elements of data to form a cohesive story and a cogent profile regarding an individual, entity, or an issue. This is the point at which risks are detected and evaluated for communication and discussion.

In reporting results to the consumer of intelligence, it is critical to consider a number of factors, including, but not limited to:

- The position, title, and roles and responsibilities of the consumer in the organization
- The country in which the consumer is located
- The relevant industry or sector with which the consumer is located
- The consumer's experience with or knowledge of corporate intelligence and due diligence
- The consumer's awareness of risks in the sector or industry in which risks are being evaluated

An example to illustrate consideration of these factors is when, for example, a corporate intelligence report assessing risks of relationships or links between a U.S.-based company and the U.S. government is prepared for a consumer of the report in a foreign country, especially a developing country. The consumers in a developing country will not necessarily understand or appreciate risks of government or political relationships or both as they pertain to the United States.

Clear, concise reporting is also necessary to ensure that those consumers who are unfamiliar with specific legal, accounting, technical, or industry-specific terminology understand the issues and risks uncovered through corporate intelligence. Succinct reporting is also important for consumers who are high-level executives and board members who do not have time to read and consider any lengthy work product.

COORDINATION AND SELECTION OF MANAGEMENT AND EXTERNAL ADVISORS FOR INTELLIGENCE GATHERING

Organizational decision making often involves a large cross-section of senior management, internal business units, and external advisors. Input on a matter arrives from the organization's board; C-level executives; general and outside counsel; finance and accounting teams; key investors and shareholders; marketing and strategy departments; human resources, and other interested parties. Therefore, it is necessary to involve all of them in the formulation of a bespoke intelligence remit not

only to ensure all relevant questions are included in the overall inquiry, but also to encourage the participation of all parties in the collection process.

Corporate intelligence is predominantly conducted by external, specialized consultants who have made the requisite investments in information systems, experienced personnel, and global networks. Both large, global consultants and small boutique advisors are renowned for their ability to seek out relevant information about clients and customers. Some specialist consultants focus on certain industries or geographies. Others have special linguistic capabilities that may be critical to an assignment. The selection of external consultants is therefore a key factor in successfully obtaining the information required.[24]

A team of corporate intelligence professionals working side by side with forensic accountants and internal counsel or external attorneys is considered to be the most effective combination of personnel to advise businesses in high-stakes transactions, internal inquiries, disclosures, disputes, compliance, and post-event remediation.

TIMING OF DEPLOYMENT

Increasingly, outside specialists and internal corporate intelligence units (in the few organizations that have them) are involved at earlier stages in the decision-making process and design of an intelligence remit. The sooner the participation of corporate intelligence experts in this process, the more successful the outcome.

These experts can help to manage expectations of the decision makers regarding the anticipated products of intelligence and the estimated timeframe required, articulate the most appropriate methodology, and highlight certain limitations of the process.

Though there is no strict rule that governs the point at which the collection and analysis process should be launched, there are certain benchmarks that guide the deployment of an intelligence strategy. For example, for the overt corporate intelligence in the context of a merger or acquisition, officially, "The process kicks off when both buyer and seller sign a letter of intent, or term sheet, which starts the purchase price for a deal. By signing the letter, the seller agrees to open up his or her own company to a top-to-bottom audit and adjust the sale price on the audit's findings."[25] However, if a party intended to launch a surprise, hostile bid against another company, corporate intelligence efforts would start confidentially and discreetly well before the bid was launched.

LIMITATIONS OF AND INHERENT BARRIERS TO CORPORATE INTELLIGENCE

Though corporate intelligence has matured in its ability to meet the expectations of its consumers, there remain numerous challenges and conflicts that arise from

[24] Scott Moeller and Chris Brady, *Intelligent M&A: Navigating the Mergers and Acquisitions Minefield* (West Sussex, UK: John Wiley & Sons, 2007), 85.
[25] Moeller, *Intelligent M&A*.

a relatively limited understanding of the intelligence-gathering abilities and related processes.

Misguided Assumptions Regarding Database and Electronic Research

First and foremost, there exists a common and fundamental misunderstanding regarding the capabilities of electronic and database research. "One of the great fallacies that has spread rapidly over the past several years is the myth that somewhere out in cyberspace there is a 'Great Database in the sky,' a huge central repository that can be tapped into and, voila, instant answers appear miraculously on the computer screen. Many also believe that since the Internet is a free service, they can get instant access to any information they want at no cost."[26]

Another misunderstanding regarding corporate intelligence is the reliability of information produced by electronic research. "The Internet is a repository of public information, and most of that information is posted by people and companies that want you to know about them. It's a form of advertising. The information, therefore, may be exaggerated or misleading, because there are no controls over the accuracy of it, and as we well know, people are prone to try to present themselves in the best light possible, even if they have to fib a little."[27]

A CNN story from March 11, 2010, exposed the limitations of purely online, or automated, background checks and the potentially fatal consequences of those deficiencies. The story opened, "A background check conducted in 2009 on an Ohio State University employee suspected of opening fire Tuesday on his co-workers turned up no criminal record, even though he apparently served five years in prison." As reported by CNN, two separate vendors of online criminal records did not return results of criminal history for Nathaniel Brown, who had apparently applied for a job as a janitor at the school. These findings were contrary to the fact that Brown had spent five years in prison.[28]

Marginal Treatment of Corporate Intelligence Advisors

Too frequently, a corporate deal team does not inform or suitably include their general counsel or compliance officers until the last minute, which is mostly attributed to the team's desire to guard sensitive deal information.

Even in organizations that have a nominal business intelligence function, M&A groups may engage the intelligence staff only as bare data providers, and at the last minute. As such, they may become disengaged and even obstructive. Interviews with business intelligence staff confirm this and also confirm that they sometimes feel undervalued and peripheral to an important business transaction.[29]

---

[26] F. W. Rustmann Jr., *CIA, Inc.: Espionage and the Craft of Business Intelligence* (Washington, DC: Potomac Books, 2002).
[27] Rustmann, 82.
[28] "Background Check Missed Suspect Shooter's Prison Stint," *CNN Justice,* March 11, 2010.
[29] Moeller, 143.

Pressures on Corporate Intelligence Teams

Corporate intelligence is not produced in a vacuum. Many interests are at play in high-level decisions that can affect the intelligence-gathering-and-analysis function. This is especially true in business, when the decision is tied to predetermined incentives based on a certain outcome, such as a successful acquisition.

In the case of a transaction, some of the most common pressures on corporate intelligence are deal momentum and personal interests. One mining industry executive cited the forces of individuals' personal credibility or job promotion riding on a deal. These individuals are often encouraged by their own desire to succeed to ensure that a deal doesn't fail as a result of uncomfortable information that can be derived from intelligence gathering and analysis.[30] Deal teams, therefore, can become hesitant to engage a corporate intelligence advisor to obtain information on people, entities, and issues related to a particular transaction.

Other frequently encountered constraints are limited time and budget allocated to produce and analyze intelligence. Because corporate intelligence is still a relatively marginal function in the overall strategic decision process, the required time and resources are not always anticipated. Lacking appropriate money and time, an intelligence function can be severely crippled to the point of being entirely ineffective, especially when the subjects of an inquiry are complex and located in less transparent jurisdictions.

LEGAL PARAMETERS AND OPERATING CONSTRAINTS VERSUS ENABLING LEGISLATION

Because intelligence gathering is an inherently invasive and sometimes controversial process that involves securing and handling sensitive information, there are strict legal and ethical frameworks that regulate the function. These are most applicable in instances when the corporate intelligence process requires discreet collection methodology, but are also relevant in consensual due diligence processes. As concerns regarding protection of intellectual property and personal information have risen, so, too, have the protective measures.

Most of the legal parameters are those that generally govern private intelligence and investigation.

The U.S. Economic Espionage Act

The Economic Espionage Act is a prominent restraint on the general practice of private investigation and intelligence gathering for commercial purposes. The law applies mostly to a function that focuses on gaining insights regarding the competition. Because businesses have suffered significant economic losses because of breached confidential information, any intelligence process that involves collection of sensitive commercial data and material may fall under the purview of the Economic Espionage Act.

[30] Moeller, 143.

The Act is "one of the most significant pieces of criminal intellectual property legislation in history, designed to combat the theft of American intellectual property by foreign governments and foreign companies."[31] This legislation is concerned mostly with the protection of trade secrets, but the broad definition can include all forms and types of financial, business, scientific, technical, economic, or engineering information. Since corporate intelligence can seek to secure and analyze organizational information that falls under many of these categories, it is critical to ensure that a collection and analysis methodology is compliant with provisions of the Act. Compliance considerations are especially important when the intelligence benefits a foreign entity or individual and the subject of the inquiry is a member of the U.S. private sector.

Telephone Records and Privacy Protection Act of 2006: Anti-Pre-Texting Legislation

Pre-texting is loosely defined as the act of creating an invented scenario or identity as a maneuver to persuade a victim to release sensitive information or perform a particular act that benefits the deceiver. Until January 2007, when pre-texting to secure confidential information was formally criminalized in the United States through federal legislation, it had been a popular method used by less scrupulous private investigators and intelligence practitioners to obtain highly sensitive information on an individual or company. Though the use of pre-texting has abated in the United States, it remains a prevalent method for less ethical practitioners in overseas territories.

In 2006, Hewlett-Packard (HP) became the subject of a major controversy when the company's leadership and security department retained a private investigator to identify the HP board member who was suspected of leaking confidential information to the press during the course of an internal board dispute with management. The contracted investigator reportedly used a pre-text to approach a telephone utility company so he could secure the targeted board member's personal phone records, which confirmed that he was having conversations with a journalist. The incident spawned a flurry of state legislation to outlaw pre-text methods, and the federal government followed with the enactment of the Telephone Records and Privacy Protection Act, signed by then-President Bush in January 2007. The first prosecution of criminal charges under the newly enacted anti-pre-texting legislation following the HP incident occurred in January 2009. An Ohio man was indicted for using a fake U.S. District Court subpoena to secure phone records from Sprint/Nextel.

Pre-texting and other forms of misrepresentation used to gain information are not considered viable approaches for corporate intelligence units that abide by legal and ethical standards, regardless of the jurisdiction.

Privacy Laws and Initiatives

Resulting from a spike in identity theft and other information breaches, many nations have enacted strict laws and regulations surrounding the solicitation and handling

[31] Hedieh Nasheri, *Economic Espionage and Industrial Spying* (Cambridge: Cambridge University Press, 2005).

of personal information. Provisions influence the use of personal information for legitimate purposes, ranging from pre-employment screening to credit checks to due diligence.

For example, in the United States, the Fair Credit Reporting Act, originally passed in 1970, has gained new prominence as the sharing of personal information has become controversial in the United States. The Act is meant to regulate the collection, dissemination, and use of consumer information, including consumer credit information. This regulation is especially pertinent to corporate intelligence because this act restricts many of the databases that corporate intelligence professionals use to conduct research on individuals from providing fully identifying information. Lexis-Nexis, WestLaw, Choicepoint, eFunds, and others are all required to redact particular identifiers in order to protect an individual's credit information. Similarly, the Act applies to any company or individual that secures personal identifiers from public records.

The Safe Harbor Act, also known as the European Union Data Protection Directive, enacted in 1998, similarly protects the personal information of citizens in European Union member countries. The Act prohibits the transfer of personal data to entities and individuals outside EU member countries that do not meet the European adequacy standard for privacy protection. Therefore, corporate intelligence products containing personal information of EU citizens that is submitted to individuals outside of the European Union must be appropriately treated so that reporting does not violate the Act.

The increase in accessibility of public records from the Internet has caused growing concern among citizens in the United States that personal data on such records, such as UCC filings, would be accessible for abuse or theft. After a number of lawsuits were filed by citizens against state governments for publishing personal information on electronic public record sites, several states began to systematically redact such data from public records. In California, for example:

> *The state began a comprehensive effort in early 2007 to redact Social Security numbers in UCC filings. . . . California has about 2.3 million filings (6.6 million images) that are the focus of redaction efforts. . . . Secretary of State Debra Bowen has worked with the state legislature to address these shortcomings of UCC information policies. Assembly Bill 1168, which takes effect in January 2008, requires the secretary of state's office to redact at least the first five digits of Social Security numbers from UCC filings.*[32]

While the laws serve to improve protections afforded to individuals, these laws and regulations in combination have created new challenges for corporate intelligence professionals to secure detailed background information, especially on individuals.

---

[32] "Privacy, Public Access, and Policy-Making in State Redaction Practices: Dealing with Sensitive Data in an Era of Open and Accessible Public Records," National Association of Secretaries of State (NASS), National Electronic Commerce Coordinating Council (eC3), December 2007.

Enabling Legislation and Regulation

As much as certain privacy and intellectual property protection laws have created challenges for corporate intelligence gathering, transparency laws and regulations have also enabled intelligence practitioners to access critical records, enabling research, corroboration, and validation in the information collection and analysis process.

The U.S. Freedom of Information Act (FOIA) is a powerful legislative tool that ordinary citizens can use to compel the release of information from public records. Signed into law by President Lyndon Johnson in 1966, the Act requires the partial or full release of records and information controlled by the U.S. government. Thirty years later, in 1996, the Electronic Freedom of Information Act required that the government make certain documents and records available electronically, which broadened the online access to government records. Though the breadth and depth of the Act's mandate has fluctuated because of national security and foreign espionage concerns, the general trajectory is that FOIA has permitted the disclosure of an increasing number of records.

Other examples at the U.S. federal level are increased disclosure requirements of hedge funds with Form ADV.

At a state level, sunshine laws prescribe that state governments provide access to a wide variety of public records. Some states' transparency mandates are more potent than others. Florida, for example, is a state that mandates a high level of public disclosure, requiring that numerous state records be electronically accessible. Delaware and other states considered as tax havens and to be corporation-friendly have not yet enacted sunshine laws that are considered to be as demanding.

While the United States has benefited from FOIA and sunshine laws since accelerated implementation in the 1960s and 1970s, this trend is even more remarkable in traditionally nontransparent foreign jurisdictions. Governments in these territories seeking to foster investment-friendly environments have taken measures to require new levels of disclosure and information registration. Colombia, for example, a country with a long history of institutionalized corruption, recently enacted a law in 2007 requiring election campaign candidates to maintain and register their donations and campaign treasury bank accounts through an adopted program called *cuentas claras*. Mexico, also known for criminal corruption, recently made criminal records available through the Lexis-Nexis database system.

The domestic and international strides in transparency are important to recognize as they facilitate increasingly efficient and effective corporate intelligence operations.

ETHICAL DEBATES SURROUNDING CORPORATE INTELLIGENCE

New ethical standards are partially credited with advancing the legitimacy of corporate intelligence. As companies increasingly engaged external advisors and established international corporate intelligence divisions, the discussion regarding ethical considerations began to emerge in the early 1990s. Many practitioners continue to justify the means by the end, however, especially in cases in which invasive corporate

intelligence serves to uncover or confirm suspected reputational issues in the process of due diligence.

In a paper published in the *Journal of Business Ethics* regarding a study of ethical practices pertaining to business intelligence, the author states it is:

> *. . . important for the firm to properly supervise its business intelligence contractors. The contractors should be required to abide by the same code of conduct and ethical standards that is imposed on management and employees. A firm cannot hire a contractor, be it a private investigator or a business data collection firm, and divorce itself from the methods used to fill this contract. A firm's statement that it was not aware of its contractor's actions does not absolve the firm from sharing in the responsibility for these unethical practices.*[33]

Questions that surround corporate intelligence are often complex. Examples are:

Can a firm request one of its vendors to provide intelligence on the subject of an intelligence inquiry, knowing that the vendor is well-positioned to comment on the subject?

Is it possible to ethically approach a subject's customers as targets for intelligence inquiries, as they are well positioned to secure insider information, and do these customers have a duty to safeguard that information?

Can external intelligence advisors provide intelligence for a client regarding an entity or individual for which or whom it has worked in the past?

A recent, highly visible lawsuit between a consultancy providing corporate intelligence services and one of its clients demonstrates the need for rigorous ethical judgment in accepting and managing such matters.

In 2009, a risk management consultancy was sued by one of its clients regarding pretransactional due diligence services that the consultancy had provided to its client for an investment consideration. The client demanded damages from the consultancy after it lost its multimillion-dollar investment in a financial services company that proved to be nothing more than an elaborate fraud scheme. In its due diligence services provided to the client, the consultancy allegedly failed to identify major issues that might have deterred the client from making its investment. However, the client did not sue purely because of the consultancy's failure to identify red flags in the investment target. Rather, in the filed complaint, the client alleged that the consultancy did not disclose that there were possible "conflicts of interest" at the outset of the engagement. According to the complaint, the consultancy had a business relationship with the fraudulent entity and its CEO. The civil case was eventually settled out of court for an undisclosed amount. This demonstrates that business intelligence consultancies must be careful to identify and disclose any material relationships they might have with the subjects of their due diligence.

---

[33] Norman O. Schultz, Allison B. Collins, and Michael McCulloch, "The Ethics of Business Intelligence," *Journal of Business Ethics* 13(4): 305–314.

SUMMARY

With constant evolutions in the features of the global marketplace, the need to refine the tools for mitigating risks and combating fraud and corruption is ever present. From its sixteenth-century origins in the East India Company's scouting missions as a means to identify opportunities in newly discovered lands, corporate intelligence now stands as a set of methods that protect the integrity of the world's legitimate commerce and capital market system.

While the basic legal and regulatory frameworks governing global commerce are the main drivers behind corporate intelligence, company leaders are beginning to recognize the cost efficiencies and the inherent business value of being better informed before making important decisions. Like forensic accounting, corporate intelligence is a practice that can be adapted and scaled to not only address a range of serious business risks, such as fraud and corruption, but also support other areas of strategic decision making. Its flexibility permits it to serve in a preventative or compliance capacity to facilitate enhanced due diligence or market entry studies, as an investigative instrument to focus on subjects of internal inquiries or multiparty disputes, and as a component of a remediation plan after the occurrence of an incident.

Corporate intelligence practitioners and forensic accounting experts will find the combination of the distinct qualitative and quantitative skill sets to be the most robust approach to identify and mitigate risks, interrogate the facts of an alleged circumstance, or rectify the aftermath of a negative event.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 16

The Art of the Interview

Thomas W. Golden and Michael T. Dyer

An interview is a conversation with a purpose. The purpose is to obtain information and, in some cases, an admission. Experienced forensic accounting investigators know that the great majority of white collar crimes are solved by a skilled interviewer, not by other forensic means. Arguably, there is no more compelling proof of a crime than a perpetrator's voluntary admission.

Effective interviewing is an art to be studied, a skill to be honed. In the later twentieth century, interviewing also emerged as a science, drawing on decades of psychological and sociological research, including a great deal that had been learned from wartime interrogation. Volumes of scholarly research exist, and more are published each year. Yet whatever scientific techniques are brought to bear—Gudjonsson's cognitive-behavioral model of admission, for example, or Reik's psychoanalytic model of admission[1]—in the end, the interview process itself is a subtle art that draws on the experience and skill of the practitioner.

The interviewer must plan effectively beforehand, approach the session with a variety of tools and tactics to choose among, follow a line of questioning, evaluate its effectiveness as the interview proceeds, and, if necessary, move seamlessly to a new approach. Effective interviewing is more than a well-executed analytical exercise; it requires great sensitivity to the subject's feelings and thoughts.

Interviewing skills must be developed. The best way to develop them is to sit in with or observe experienced interviewers at work. Some courses provide excellent training in conducting interviews, but just as learning to drive a vehicle requires considerable road time, so interviewing requires conducting interviews with an experienced mentor close at hand. After the interview, interviewers should critique how it went, summarize what was learned, focus on what could have been learned more quickly, review where the questions flowed smoothly and where they disrupted the flow, take note of what leads were developed, and discuss any key questions that went unanswered or, even worse, unasked. Interviewers must learn to hear and see what works and what does not and must learn from successes and failures.

There is no one right way to conduct an interview. Inducing someone to make an admission is a difficult task indeed. The interviewer must be prepared to

[1] David E. Zulawski and Douglas E. Wicklander, *Practical Aspects of Interview and Interrogation,* 2nd ed. (New York: CRC Press, 2002), 12–13.

assume a variety of stances, moods, or roles. Interviewers can be sympathetic, logical, confrontational, accusatory, or intimidating. Generally, in dealing with white collar criminals, intimidation is less successful than the softer, sympathetic approaches, but that does not mean that a hard line is never appropriate.

DIFFICULTY AND VALUE OF OBTAINING AN ADMISSION

Later, we describe the different types of interviews that a forensic accounting investigator will encounter; however, note that the admission-seeking interview is the most challenging of interviews and requires substantial skill on the part of the interviewer. The interviewer must quickly evaluate the success of the line of questioning and be prepared to move seamlessly, if necessary, to a new strategy and another line of questioning. The interviewer must evaluate what may persuade the witness to provide information that the witness has no intention to disclose. The success of an interviewer depends more often on the ability to craft a persuasive argument than the ability to craft precise questions. Remember the opening sentence to this chapter: An interview is a conversation with a purpose. The good interviewer constructs a line of questioning interspersed with selected commentary and documents in an attempt to induce the subject to confess. Simply crafting a line of questioning without regard to building a persuasive argument quickly turns into a note-taking assignment unlikely to benefit the purpose of the investigation.

Even highly experienced interviewers know that it is extremely difficult to get someone to admit to a crime. Go back to your early years as an adolescent, or recall instances with your own children. The car has a mysterious dent in it. The window is broken. You were caught cheating on an exam. You know you did something wrong, you feel guilty about it, and the last thing you want is to be discovered. Your dad comes to you asking about the dent in the car, and your first reaction is, "What dent?" You do not want to lie; you just want to deflect the question. You want to keep deflecting until he drops the issue. If he does not let it go but keeps coming at you, he slowly decreases your desire to continue lying. If your dad is good at getting to the truth, he says things that increase your desire to tell the truth. "Son, I know you didn't mean to do it because you are a good kid. If you caused the dent, now is the time to discuss it."

In most investigations, obtaining an admission can be of significant benefit to the overall objectives of conducting an investigation, especially when the client wishes to refer the matter to a prosecutor. (See Chapter 19.) There is no one successful strategy—hence, the title of this chapter, "The Art of the Interview." Keep in mind that we are usually not dealing with a hardened criminal but, rather, with someone who fits the profile of a typical white collar criminal. (See Chapter 2.)

Incorporating a sequence of interviews into an investigation can be a costly strategy, but the value of obtaining an admission cannot be underestimated. An admission can go a long way toward ensuring a successful prosecution should a referral be made to a prosecutor.[2]

[2] As discussed in Chapter 19, the prosecutor will determine if a matter is worthy of prosecuting. Such actions are not made for the benefit of an individual or corporation.

PLANNING FOR THE INTERVIEW

In preparing for the interview, a number of important issues must be considered. A good starting point is the question of what the interview subject is likely to know. Solid investigative work and previous interviews can help the forensic accounting investigator focus on the subject at hand, develop a line of questioning designed either to carry the investigation forward or to elicit an admission, and contemplate what approach is likely to be the most effective. Among the issues to consider are the following.

- *Timing.* The forensic accounting investigator must ensure that there is adequate time for a thorough interview. If the subject says, "I can drop by from 4 to 4:30, but then I have to pick up my kids," the interviewer should schedule another time. The interviewer must insist on adequate time and resist any suggestion that the interview be spread out over several sessions.
- *Location.* Ultimately, the forensic accounting investigator must conduct the interview at whatever location the subject insists on, but whenever possible the interview should be conducted in a business environment that can be controlled. The ideal setting is a room with few distractions: no windows to look out, no clock, no photos, books, or model airplanes. The goal is to create an environment in which the subject has nothing to look at except the interviewer and that makes clear to the subject, not so subtly, just who is in control. The forensic accounting investigator should plan to seat the subject facing the interviewer or interviewers, with a plain wall behind the interviewer. When possible, the interviewer should sit between the subject and the door. Of course, the subject cannot be held against his will, but if the subject wants to walk out, the layout of the room should make that act as uncomfortable as possible for the subject.

  On the other hand, the forensic accounting investigator must be flexible. If the client no longer employs the person being interviewed, the interview is likely to take place outside the office. The forensic accounting investigator should offer to go to the subject's residence or place of employment but be prepared to conduct the interview even in a car or at the mall. The forensic accounting investigator should not let a disagreement over location become an obstacle to gaining information.
- *Legal issues.* Interviews, and especially admission-seeking interviews, may raise certain legal issues and may expose the company and the forensic accounting investigator to certain risks, one of which is a defamation lawsuit. The forensic accounting investigator should proceed only after consulting with counsel. A lone, zealous forensic accounting investigator should not go off on her own. The forensic accounting investigator should seek and obtain team decisions.
- *Recording.* Whether to electronically record interviews is a matter of some debate. Recording an interview works against the goal of lowering the subject's defenses. While federal law does not preclude such recordings, you may be in violation of state law if you decide to record an interview covertly (if only *one* party is aware that the conversation is being recorded—in other words, if the forensic accounting investigator records without the interview subject's consent). Some states permit covert recording of an interview, and others do not. Many states

require that both parties consent to the recording. A recorded interview can be a powerful negotiating tool in settlement talks. Many factors must be considered before deciding whether or not to record an interview, including state law, the forensic accounting investigator's experience, and the advice of counsel. If you are working at the direction of law enforcement or under a 6(e) order, you may be subject to different restrictions. In some jurisdictions employees may have control over the question of whether to record pursuant to local labor law. They may, for example, have the right to record the interview for their purposes if they want.

- *Polygraph*. The Employee Polygraph Protection Act, passed by Congress in 1988, does not allow private employers or their representatives to require employees to take a polygraph, with few exceptions. It also prohibits employers from disciplining or discharging employees who refuse to take the test.[3] Many commentators have suggested that the law should be interpreted to forbid forensic accounting investigators from asking employees if they are willing to take a polygraph. Whatever the appropriate interpretation of the act, forensic accounting investigators should leave this tool to law enforcement and other government authorities.
- *Participants*. Two people should conduct most interviews. The interview will proceed more smoothly and with fewer gaps if one interviewer asks questions while the other takes notes. Of course, the interviewers can switch roles, but the second interviewer should primarily observe the behavior of the interviewee and consider what questions that behavior suggests. When interviewers work together over a period of time, they learn each other's pattern of interviewing. The second interviewer might step in to fill a pause in the interview while the primary interviewer gathers next thoughts. The second interviewer also provides a witness for any admission that emerges, as well as for any disputes about the conduct of the interview.

  In some cases, it quickly becomes clear that the primary interviewer and the subject have a personality clash. Switching interviewers may ease the tension and lead the subject to open up. This has been termed the good cop/bad cop scenario, with the good cop providing a more sympathetic ear and reducing the tension created by the hard-nosed approach of the bad cop. For this approach to work effectively, the two interviewers need to coordinate beforehand their goals and tactics.

  A forensic accounting investigator must be cautious when working with an unfamiliar partner. What one person perceives as a gap in the interview might be a deliberate silence created by the first interviewer. Or the second interviewer may believe that the primary interviewer missed a question, when in fact he was holding it in reserve. Let your partner know that at a certain point in the interview, you will turn it over to him to cover the possibility that you missed an important question. You will now have a second chance to pose that question through your partner. A good exchange would be to simply turn to your partner

[3] *Admissibility of Confession as Affected by Its Inducement through Artifice, Deception, Trickery or Fraud,* American Law Reports 2d, 772 (Rochester, NY: The Lawyers Cooperative Publishing Company, 1965), 69–70.

and ask, "Do you have any questions?" It is a good practice for interviewers to excuse themselves from the room at certain times or just prior to concluding the interview in order to compare notes privately and thus ensure that all relevant topics have been addressed.

- *Multiple interview subjects.* Forensic accounting investigators should never interview more than one person at a time. Even with two employees from the same department, forensic accounting investigators should interview them separately, and at best consecutively, so that one cannot tell the other anything about the interview. Separate interviews provide the best opportunity to draw out a subject and to ensure that one person's statements are not influencing the other's.
- *Concurrent interviewing.* When more than one person must be interviewed, it is sometimes useful to conduct the interviews simultaneously and use information obtained in each interview in the other. The interviewers need to be in touch with each other, perhaps through a phone call, e-mail, or instant message suggesting a quick meeting in the hall.

TYPES OF INTERVIEWS

Interview planning must reflect the type of interview that is anticipated. For the purpose of this chapter, all interviews are divided into two categories: information seeking and admission seeking.

The Information-Seeking Interview

Not everyone interviewed in an investigation is a suspect. Some individuals will be interviewed because they have information about the company, the industry, or the accounting at issue. Such interviews are necessary parts of the investigation, providing knowledge that will sustain further inquiry. In most investigations, the forensic accounting investigator starts interviewing at the periphery of all possible interview candidates and moves toward the witnesses appearing more involved in the allegation that is the subject of the investigation. (One useful technique is to interview people on the periphery and then watch to see if anyone comes along to inquire of them about what questions were asked. Individuals who are particularly curious about the goings-on of the investigation should receive attention.) The more pertinent the information obtained during information-seeking interviews, the more likely it is that the admission-seeking interview will be successful.

The information-seeking interview is usually nonconfrontational and not particularly stressful, but the interviewer should never assume that such interviews are unimportant. In some cases, the interview subject may provide the only evidence available.

The interviewer must prepare for witness interviews by forming and assessing various theories about what has occurred, yet the interviewer must always be open to new possibilities. Remember, too, that while forensic accounting investigators are trained at asking questions, the various witnesses are most likely *not* trained in providing answers. Even if they are cooperative, they may not be efficient and may not be aware of what information is important. The forensic accounting investigator's challenge is to draw data out with the right questions. It is rare for a witness to provide

all of the information sought without the help of probing questions. A common tactic of fraudsters is to give honest but incomplete answers, and innocent witnesses may also have difficulty assembling full sets of information for the interviewer. For this reason, forensic accounting investigators must be very good listeners.

The interviewer must also beware of making assumptions. (See Chapter 12, where this is identified as a common misstep.) Most intelligent people prefer not to ask dumb questions. Instead, they make assumptions, but this is not a good idea during an investigation. The interviewer should not be afraid to ask many questions, even when the answers may be obvious. And the interviewer should not be afraid of sounding dumb. Ask for whatever information is needed, more than once, of the same person, of different people, and take good notes.

The Admission-Seeking Interview

This is the most challenging of interviews. It requires substantial skill to complete successfully. In planning the interview, the forensic accounting investigator should be confident that the witness has committed the crime under investigation or has knowledge of the illegal act. The interviewer must consider what may persuade the subject to provide information the subject has no intention of relinquishing. As noted earlier, a successful interview more often depends on the interviewer's ability to craft a persuasive argument than on the ability to craft precise questions. Some experts define this characteristic as the ability to be a "confident negotiator."[4]

Even in cases in which guilt can be established through evidence and testimony from others, an admission is extremely useful because the suspect may admit to acts previously unknown to the forensic accounting investigator and is likely to be more cooperative in any subsequent civil, criminal, or administrative action. An admission may also make a trial unnecessary.

To extract an admission of guilt, interviewers may need to make clear that they know the suspect is lying. People react to this accusation in different ways: some become emotional, break down, and confess everything; some respond aggressively; others grow silent. Experienced interviewers know they must first find ways to obtain an initial admission of wrongdoing and then continue questioning to expand that admission into all pertinent areas. To be successful, the interviewer must be well versed in and comfortable with a variety of approaches, including the following:

- *The logical approach.* This direct approach begins by laying out the evidence of guilt that has been found and explains the futility of not confessing. "If I committed a crime and there was no evidence," the forensic accounting investigator might say to the suspect, "I would not make any statement. But here, because we have adequate evidence of your guilt in the accounting records, it is to your advantage to appear to be cooperative, and this statement will demonstrate a willingness to cooperate. Tell us your side of the story. It will be difficult to maintain in the future that you were cooperative in resolving this matter if you are not cooperative now. Maybe someone else who knows what

[4] Id., 38.

you know will come forward and cooperate with us. Then, what information you may decide to disclose to us at a later time becomes much less important. The value of the information you have about these accounting records has a short half-life. Disclosing now what you know may be your best course of action."

This logical approach may start the suspect talking, which is always a good sign. Major admissions often start with small admissions. Sometimes the witness grows so comfortable talking that the ultimate admission includes admissions of additional improprieties of which forensic accounting investigators were unaware.

- *The do-the-right-thing approach*. During preparation for the interview, if the forensic accounting investigator learns that the interview subject had a history of doing the right thing, that information can be used to appeal to the subject's feelings. As we discussed in Chapter 2, the profile of most white collar criminals fits that of people who, but for a situational experience or misguided rationalizations, by and large have lived normal lives in which doing the right thing has been a way of life. Reminding them of this commonly held belief oftentimes evokes a willingness to revert to that behavior.
  - "I know your family raised you to do the right thing."
  - "You were a Marine. You know how to accept the responsibility of citizenship. You know what honor means."
  - "Your dad was in law enforcement, and he taught you to do the right thing."
- *The silent approach*. When two people are engaged in conversation, silence almost always makes one of the individuals uncomfortable. To relieve the uncomfortable feeling, someone usually begins to talk. Silence often makes interviewers uncomfortable to the point that they even suggest answers to the suspect! Do not fall into this trap. Make silence work for you, not against you. Here is an example:

  Interviewer: I am here to ask you if anyone that you report to has asked you to make journal entries or other accounting entries that made you uncomfortable.

  Witness: No response.

  This question could cause the subject to pause and ponder over a response, especially if the subject actually is aware of an event that may be an indicator of fraud.

  No matter how long it takes to get an answer, wait. After a period of time, perhaps two minutes of silence, you may repeat the question. Whatever you do, do not let the silence prompt you to relieve it by saying something like the following:

  Interviewer: If that's not the case, then just say so and we'll move on. I don't mean to imply that there's anything going on here [*and on and on . . .*].

  Silence is a powerful tool. Use it well and use it often. After you ask a question, stop talking and wait for a response.
- *The rationalization approach*. The interviewer's effort in this approach is to give the subject a moral or psychological excuse. Helping the witness place the crime into a rational context—one implying that others similarly situated would do the same thing—can unlock the needed admission.

In Chapter 2, we discussed the three ingredients that enable someone to commit a financial crime: need, opportunity, and rationalization. The third ingredient, rationalization, offers the basis for an effective interviewing tactic. Let's say that the suspect is withholding information. By identifying with the suspect, the forensic accounting investigator may prompt the suspect to talk. Many white collar criminals are truly sorry that their fraud and cover-up have caused trouble internally or harmed investors. Because they believe that they are good people at heart, they rationalize what they have done. The forensic accounting investigator should be sympathetic, and help the suspect recreate and articulate the rationalization.

"I'm sure you were angry when Bill got the bonus you should have received," the interviewer might say. "I know you're one of the major reasons this business became successful, and you were grossly underpaid. I understand why you felt they owed you money." A suspect who is feeling guilty may want to get it off his chest by telling someone empathetic why he committed the crime. Helping someone arrive at what might appear to be a rationale for his or her actions allows the subject to save face. "Anyone in your situation would have done this; everybody makes mistakes," the interviewer might say. The interviewer's mission here is to give the subject an acceptable reason to come clean.

In one example, the interview witness was an individual who had created a series of falsified journal entries having the effect of increasing financial statement income. The forensic accounting investigators believed that at least part of the motivation for the falsification was to meet the requirement for an annual bonus: Were the individual to achieve division sales of $20 million, a bonus equal to his annual salary would be paid to him. One dollar less and there would be no bonus. Various interview techniques had failed. The perpetrator avoided making any admissions until it was proposed by the interviewer that perhaps part of the reason for the falsification was to protect other employees at the company from possible loss of their jobs should the division fail to meet budget. Apparently, the witness turned out to have been hankering for a noble motive to rationalize his illegal and selfish act. He admitted to falsification of the financial statements because he could now justify the act as an effort to protect fellow employees. The rationalization approach is often successful because it allows the subject to save face during the interview.

- *Asking questions to which you know the answers.* This approach is best to determine a subject's credibility. Its effective use early in the investigation could save countless hours in blind alleys. If you can determine the validity of what someone says at the moment the person says it, the investigation can be structured much more efficiently and is likely to yield a much better result.

  Lying about an important matter is not easily rationalized. If you come across someone who has the ability to rationalize lying to you, then you may have found someone who quite possibly has been lying for quite some time. If you are interviewing someone whom you have just caught in a lie, regardless of the context, as soon as you practically can, focus on the allegations that triggered the investigation.

  Alternatively, you can review documents and conduct a host of other interviews in search of something to support the initial allegations. However, asking the right questions of the right person at the right time in the investigation could

save your client time and money. Remember: Liars lie. Find a liar, and you may be well on your way to finding criminal activity.

Forensic accounting investigators must always bear in mind that a method successful with one subject may be ineffective with another. The interviewers must be nimble enough to evaluate whether a strategy is working and to abandon it for another when it is not. They must remain flexible, acknowledge mistakes and false starts, and never lose sight of the objective: to obtain information and, ultimately, an admission.

One approach not yet discussed is to bluff. Bluffing almost always fails, and our advice is to never bluff. It is also important to note that interviewers are *not* permitted to use coercion or duress. Consult counsel for definitions, but here is an example of coercion: "I know you stole the money, and if you don't admit it, I will tell your employer and you'll get fired." And here is an example of duress: "If you don't confess, you could have an unfortunate accident on your way home tonight." Both coercion and duress are illegal.

OTHERS MAY WISH TO ATTEND INTERVIEWS

In the course of forensic accounting investigations, a number of parties are interested in what witnesses have to say. Officers and managers from the victimized entity often want to participate in the interview of a subject. They are angry and impatient to know the truth. However, it is not at all productive to have emotionally charged individuals attend. They may insist on sitting in, on the grounds that they have the facts to prevent the witness from lying; however, victims make poor interviewers. The interviewer should take the necessary time to learn the facts of the case, and on this basis be ready to determine if the witness is lying. The interviewer can deal with lying in a professional and advantageous manner. The less emotionally involved the interviewer, the more likely the interviewer will achieve the objective of the interview.

It is preferable to have no more than two interviewers conduct the interview in most situations. Others may wish to simply sit in on the interview as silent onlookers; however, that may distract the witness and create difficulties in establishing rapport and getting the witness to speak openly. There are situations, however, particularly when both counsel and forensic investigators are participating in an investigation, in which there will be more people who may need to attend certain interviews.

Forensic accounting investigators nearly always prefer to perform some level of document examination before beginning the interview process. Only after obtaining a reasonable knowledge of the company's processes and of relevant transactions do they typically begin the interviewing process, usually in a selective and strategic manner. This well-prepared approach is, we believe, critical to achieving desired outcomes. The most important leads and breaks in investigations often come from testimonial rather than circumstantial evidence; that is, facts learned in an interview are often more beneficial to achieving the desired result than documents are, which serve well to corroborate testimony. But to conduct good interviews, you still need good documents.

The interview process is clearly all-important to the forensic accounting investigator. Do the interview too early, and you could tip your hand and lose a critical

advantage. Do it without adequate factual knowledge to ascertain the honesty of interview answers, and the interview could become just a note-taking exercise that fails to advance the investigation.

INTERVIEW PROCESS

Your objective is to obtain information. You are a fact finder. Do not hesitate, therefore, to cover the basics with the interviewee: *who*, *what*, *where*, *when*, and *how*. In forensic accounting matters, you should always consider asking the interviewee what documents exist to support the information. To obtain additional witnesses, ask the interviewee if anyone else is aware of the information provided in the course of the interview. "Whom else do you think I should talk to?" People are different; one approach will not work with everyone. Be prepared to try different approaches. If you are unsuccessful with one approach, back off and try another. Just do not lose the interviewee's attention. Keep it focused on you and on the issues at hand. The interviewee needs to know that you are in control. This is *your* interview. The interviewee can end the interview at any time, but if properly conducted, the interview may well proceed along the desired lines. If an employee offers undue resistance to the interview, his employer may consider mandating cooperation as a condition of continued employment.

With these varied interview approaches in mind, let's walk through an interview step by step.

Step 1. Bonding. As a first step, the interviewers try to bond and build rapport with the witness. They advise the interviewee generally of the reason for the interview, the point being to put the subject at ease. In some cases, the interviewee knows why you are there and so may be reluctant or uncooperative. Management should consider, on the advice of counsel, various methods to ensure the employee's cooperation with the investigation, including the investigator's saying to the employee, "The company expects your full cooperation with this investigation."

At all times, be courteous toward interviewees. Remember, you are attempting to obtain information. Be friendly, sympathetic, polite, professional, and interested in what the interviewee has to offer. A condescending or bullying attitude will be ineffective. It is very important to establish rapport at the outset, especially in interviews that seek an admission, and for this reason it is usually a mistake to jump right into the questioning.

Why not begin questioning at once? Assume that you have been working with this person during the investigation. If you have been doing your job correctly, you have been friendly and cordial to the subject throughout. At the stage of the investigation where you have a reasonable certainty that the witness either has committed a crime or has knowledge that one has been committed, you want the witness's defenses to be low. You want the individual to continue to be comfortable around you. Keep in mind that most white collar criminals would be very embarrassed if someone knew of their crime. In most of these types of interviews, you will likely come to a point when you let the witness know that you know she is lying. The reactions

you expect are shame and disappointment. You also expect that the witness will be eager to win back your approval. That wish could convert into an admission if the witness feels she simply cannot go on lying and hurting people.

Does this approach work all the time? Of course not, but keep in mind that you are likely to be interviewing a person who is otherwise good,[5] although she has done something—which in hindsight she would recognize as ill-advised—and now regrets her actions. She has a tremendous sense of guilt and wishes relief from it, as if it were a physical pain. If you push the right buttons and say the right things in a sympathetic and understanding manner, you may provide just the right environment to elicit an admission. That is exactly why you want to establish rapport or confirm an existing rapport early in the interview. You will need it later on.

Step 2. Baselining. Interviewers learn from experience, and in-depth research in interviewing techniques supports the observation that putting the witness at ease with smalltalk about sports, the weather, where they are from, and so on achieves two aims. The first aim is to lower the subject's anxiety level and get him talking in a comfortable manner (as discussed in the preceding section). The second aim is to enable the interviewer to get a feel for the subject's body language, eye movements, facial expressions, and voice inflections under various stress levels. The value of observing body language, a technique used by some interviewers to draw conclusions about a witness's veracity, is supported by an enormous amount of scientific research. For example, crossing the arms or scratching the nose could be indications of lying; there is sound evidence to this effect.[6] Later, when you ask the tough questions, you may notice differences in these behaviors and others, which could be instructive as to the witness's culpability.

On one hand, the consensus among researchers is that one-half to two-thirds of all communications that take place between individuals are nonverbal, involving movements, gestures, facial expressions, and posture.[7] On the other hand, experts agree that no one behavior is a reliable indicator of truthfulness, even for a specific individual. One researcher, Paul Ekman, in *Telling Lies* (New York: Holt, Rinehart and Winston, 1981), pointed out that even when hand and arm gestures are reliable signs that an interview subject is upset, they are not reliable indicators that the subject is being untruthful.

The interviewer, however experienced, must proceed very carefully in both observing behavior and interpreting what it may mean. A body of research suggests, for example, that an interview subject with something to

[5] See Chapter 2 for a discussion on the profile of white collar criminals.

[6] The medical explanation for why someone who is lying may scratch his nose is as follows: under stress (as when someone is lying), the body's defense mechanism causes the blood to retreat toward the organs and away from the capillaries, which are near the surface of the skin. The retreat causes a tingling sensation.

[7] An extensive discussion of the wide range of verbal and nonverbal behavior can be found in *American Legal Review* (see ALR 2d 38, 106ff.).

hide will adopt a posture that appears to protect the abdomen—leaning forward, perhaps with elbows on knees or crossing an ankle onto the opposing knee. A person with nothing to hide is more likely to sit up, with feet flat on the floor and arms and shoulders relaxed. But if a subject suddenly crosses his arms during an interview, does it mean he feels insecure and is lying? Or does it mean that he feels a draft? If someone starts sweating, does it mean he is lying? Or does it mean that he wishes the air conditioning were on?

Experienced interviewers, as noted earlier, begin the interview with easy questions to set the subject at ease and to register the subject's posture, expressions, and tone of voice. Then they ask a tough question and observe whether the body language changes. But this approach should never be more than a supportive technique—used to probe for more information or an admission. The science of body language is far from precise, and so anything learned by observation has to be viewed as anecdotal rather than as a sure finding. Note, too, that an experienced con man may be confident, manipulative, and in control of his nonverbal indicators.

Step 3. Admissions and Defenses. Forensic accounting investigators want to develop a line of questioning that will cause their subjects to admit to knowledge about certain facts, procedures, policy, practices, and any deviations from them, thereby eliminating possible defenses when the time comes to state accusations. If the forensic accounting investigator knows where he wants to end up, he can lay the groundwork through a series of questions that lock the subject into a story that is wiggle free. Time spent in planning will serve well during the interview. A good rule of thumb is that the planning stage will be three times the duration of the expected interview. Before the interview, the interviewers should prepare a list of questions, consider the possible responses to each, and then determine what the follow-up questions would be for each response. Do not hesitate to ask open-ended questions such as the following. These are among the best questions to ask:

- While you were working at the organization, were you ever asked to do something that made you feel uncomfortable?
- Did you suspect illegal activities were occurring that you could not prove?
- Did you ever speak to anyone else regarding this information?
- Who do you believe would have information that would help us?
- If you could change something about this organization, what would it be?
- Is there anything else that we should have explored or that you want to tell us?

The interviewers must also consider how the witness might respond to accusations, when the interview reaches that point. Interviewers want to avoid, for example, a situation in which the witness can say, "It's true that our policies preclude unauthorized journal entries, but anyone could have made those entries without my knowledge." To anticipate this defense, the interviewers should ask questions that result in a dialogue somewhat like the following:

Q: Is it possible that someone could create journal entries to these accounts without your knowledge?

A: That would not be possible.

Q: Why?

A: Because I review an edit listing of all JEs every Friday. I would have seen it.

Q: What if you're on vacation? What happens then? Could someone make an entry that you simply wouldn't catch?

A: No way. If that happened, I wouldn't be doing my job, and I do my job. I review that edit listing every Friday and if I am away, I always see it on Monday. It's an important control mechanism, and I make sure it gets done.

This line of questioning has now trapped the subject and precluded him from using possible defenses later, when you may become accusatory. The interviewers have eliminated a possible exculpatory response to the allegation that he made unsupported journal entries to inflate revenue. They have established that no one else could have done it without attracting attention in the review process.

Step 4. Confrontation. The interviewer lays the groundwork, then brings the accusation. The goal is to make the witness feel the burden of guilt while also perceiving the interviewer as a sympathetic person in whom one can confide. The interviewer wants the subject to feel that further lying is fruitless.

"Kathy, I'm very troubled by your last comment," the interviewer says. "Actually, I'm troubled by several of your comments here today. You have been telling me that you control the deposit of all donations and that you make them all in timely fashion. Yet the minister of the Houston First Presbyterian Church told me that he gave you a $10,000 check on June 15. It never showed up in the foundation's checking account. The endorsement on the check shows that it was deposited in your personal bank account." Kathy is likely to lower her head, a shocked expression on her face. She has been found out. Her guilt is huge. That is just where you want her. You have confronted her with the fact that you know she has been lying. This will take a moment for the witness to grasp, and the immediate reaction may be total silence. Allow her to stew about her situation. This is not the time to coach her through what you believe has happened. Be silent. Do not teach the witness that you will provide explanations, when in fact you may not yet know the whole story.

Alternatively, the witness could respond aggressively to the accusation and express adamant denial. The interviewer should remain calm and retrace his steps. He should review some of the previous questions and answers. The subject's aggressive behavior may merely be a test to see what else the interviewer knows and how certain he is that the subject has done something improper. In this situation, the interviewer should stick to his plan. Repetition is his ally. Silence will work well, too. Stay on the offensive and keep the pressure on. Should the denial shift from an emphatic "no" to an explanation, an admission of guilt may be close at hand.

When the timing appears appropriate, the interviewer can help the suspect rationalize the crime. "Look, I know you to be a good person at heart," the interviewer might say. "Not one person here thinks ill of you. Everyone knows of the financial hardship you have endured lately. In similar circumstances, most people would react the way you did. You saw an

opportunity to borrow some money, fully intending to pay it back. That's what you did, isn't it?" Then let silence weigh on the subject.

"I'm ashamed," Kathy may respond. "It's true that I only borrowed the money and had every intention of paying it back."

Now the interviewer responds, "I believe you. You're an honest person, and I know what a burden this has been for you. I guarantee you, though, that if you work with me on this, you will feel better."

The interviewers have achieved their goal of getting the suspect to talk.

Step 5. The Admission. Now the interviewers should walk the subject through the facts and specific instances of the crimes. They should bring out documents and ask questions that will solidify her involvement, knowledge, and intent. They should nail down the details, although always remaining sympathetic and compassionate. They should comfort and encourage the subject. And all the while, they should take good notes and close the remaining gaps in knowledge.

When the interview is coming to a close, the interviewers should stay in character. They should not burn any bridges through inflammatory comments. They may need additional information in the future and so should advise the interviewee that they may be in touch later with more questions. The subject may recall additional facts that might help the investigation, or circumstances may change to make the interviewee more cooperative. The interviewers should ensure that the subject knows how to contact them.

During the conduct of an investigation, it is important to segregate and control all evidence until it can be examined forensically. This is a standard procedure when considering physical documents and electronic evidence, but it certainly applies to what people know, by their own experiences and actions, at the time of the start of an investigation. As such, it is important to do two things during an interview. At the end of each interview, tell the subject not to discuss with anyone the topics covered in the interview. Also, a question that should be asked of every subject is, "Have you discussed this matter or any previous interview you have had during the course of this investigation, or has anyone approached you regarding such?" People can still talk behind the scenes, but you will stop most such discussions by incorporating these two steps into your investigation.

DOCUMENTING THE INTERVIEW

In most cases, the interview should be documented contemporaneously. Between the two participating interviewers, there may be some differences of perspective. This is not uncommon. They should review their notes, and if there are material differences they should attempt to clarify with the witness when possible. They should then create a single master version of the interview and follow their document retention policy as well as any applicable laws and regulations. If direct quotations from the interviewee are included, they should be identified as such. Documenting the interviewee's own language, particularly key portions of the admission, may be helpful to those evaluating the import of the facts disclosed in the interview.

USE OF SUBTERFUGE

Subterfuge is the use of pretext or deception about who you are so that you may obtain information that may not otherwise be forthcoming. An example of subterfuge is a forensic investigator's claiming to be a bank employee. The use of subterfuge has many legal implications and should not be undertaken unless you have clear direction from counsel and confirmation about its consistency with the client's internal policies and its legality in the particular circumstances. For our part, we do not engage in this practice because we believe the detriments far outweigh any potential benefits except possibly in situations when the forensic investigator is being hired by a government body and the practice has been specifically sanctioned by the client.

More specifically, in considering whether to use subterfuge in an investigation, one should recognize that the practice may very well backfire. What happens when the forensic investigator takes the stand and is asked, "Did you lie at any time during the course of your investigation?" What would the jury's reaction be to a yes answer? And what impact would the answer have on the overall credibility of the forensic witness?

An otherwise well-executed investigation could be for naught because of the forensic investigator's use of subterfuge.

SUMMARY

Some of these interviewing techniques are broadly useful in the regular conduct of financial statement audits—for example, preparing well, questioning and listening intently, using silence to make sure you get an adequate response, and being persistent if you do not. The full scope of these techniques, however, should be considered by forensic accounting investigators who are thoroughly familiar with the full range of interviewing techniques and are capable of using them effectively.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 17

Data Mining

Analysis of Structured and Unstructured Information

Dyan Decker, Alexandre Blanc, John Loveland, and Mona Clayton

Companies create, store, and manipulate large volumes of electronic data every day. According to a study by International Data Corp (IDC), a market research firm, around 1,200 exabytes (a billion gigabytes) of digital data will be generated this year, up from an estimate of 150 exabytes in 2005.

When mined appropriately, data provide rich information that can be invaluable to a forensic investigator. This chapter discusses the importance of data mining to an investigation, highlights the differences between structured and unstructured data, and presents some leading practices on how to successfully use data mining in an investigation.

Consider some of the ways that data originate:

- The business day dawns, and each swipe of a parking pass and building access card creates a record in a security database.
- A manager e-mails his colleagues information regarding changes to the standard price list for the company's products; a server—possibly several—stores the e-mail in the manager's and recipients' mailboxes.
- A sales representative inputs activity from each of the day's sales calls, generating a record in the company's customer relationship management (CRM) system.
- An accounting clerk inputs a batch of vendor invoices, creating a series of records in the accounts payable module of the company's enterprise resource planning (ERP) system.
- A member of the information technology (IT) department copies proprietary program code to a flash drive, puts it in her pocket, and takes it with her so that she can work on it from home. Her work computer's registry creates a record of her actions.
- A manager charges lunch with a prospective client on the corporate credit card. Several systems record this transaction: the merchant's systems, the issuing bank's systems, the acquiring bank's systems, and the payment processor's systems.

These simple actions occur daily, creating data trails that might prove critical should allegations of fraud arise. The invoice input by the accounts payable clerk for a vendor who shares the same apartment building address as the clerk might become circumstantial evidence of fraud. The computer registry file showing that someone copied proprietary information to a portable device might point to intellectual property theft. Access logs, phone records, and other information routinely captured in the normal course of business often have significant value during an investigation. How one accesses, compiles, and analyzes these various data can make all the difference to a successful forensic investigation.

DEFINITION AND BENEFITS OF DATA MINING

Data mining is the process of analyzing data to discover trends, patterns, and anomalies within a data set. These trends, patterns—or exceptions to them—may be completely innocuous and can be verified as such. However, unusual transactions—those falling outside expected norms—may signal the need for an investigation by forensic specialists who can apply their experience in data mining and in investigative techniques to the overall situation.

Data mining (or data analysis) can serve many functions within a forensic accounting investigation. On some occasions, it is the main engine of an engagement. When such is the case, data analysis is typically used for highlighting potentially unusual items, trends, or patterns of behavior. More often, however, data analysis is a complementary part of a wider forensic accounting investigation that involves several other methods of information analysis or evidence gathering, including document review, physical inspection, and investigative interviews.

Forensic accountants must understand the power of data mining for several reasons:

- The best evidence in an investigation often resides in its original, electronic form.
- Given vast amounts of data throughout today's enterprises and the fact that most, if not all, business events leave numerous data fingerprints, data mining is often the most effective (and sometimes the only) way to gather needed evidence.
- Data analysis enables investigators to merge disparate data sets together and provide insights and information that would not be available through manual review.
- Application of business rules to identify suspicious transactions can be performed on large sets of data more efficiently using data mining.

How data mining fits into the timing and scope of the investigation depends on how it is anticipated to be used by the forensic accounting team. In some cases, once the method of a fraud has been established, data analysis is conducted to estimate the amount of damages. If the team knows that several branches of an organization were affected by a fraud scheme, that team may be able to compare these results with those derived from analyses of unaffected branches and after adjusting for other relevant factors, provide management with a broad estimate of the total effect on the financial statements. When such an approach is used, the comparison should be performed after the investigation has determined the characteristics of the fraud

scheme. However, in most cases, the purpose of data analysis in an investigation is to identify suspicious activity on which the forensic accounting team can take action. As such, it begins in the early phases of the investigation.

Most investigations require an iterative analysis, alternating between input from the investigation team and feedback from the data-mining process. Frequently, the results of manual inquiries made by forensic accountants need to be fed back into and incorporated in the data analysis process. For example, if inquiries show that the fraud is limited to one or two suppliers, further analysis can concentrate on analyzing transactions in those accounts.

STRUCTURED VERSUS UNSTRUCTURED DATA

While there may be myriad types of information that can be analyzed yielding valuable observations for an investigation, they can be broadly divided into two categories: structured and unstructured data. This distinction is important because these two categories of data are approached, collected, and analyzed very differently (as presented in detail in the following sections of this chapter).

Structured datasets are presented as *records* and *fields* in which each field usually contains a well-defined data point (for example, an amount or a customer name), presented consistently over and over again in each record. The most typical examples of structured data are records stored in the companies' financial systems. These could be master vendor listings, invoice details, payments, journal entries, bank statement records, credit card transactions, and so on. Outside of financial systems, some useful structured data files that can be systematically analyzed include various logs (that is, user access logs, web logs, e-mail logs, and journals created by Outlook and similar applications).

Unstructured data can take many forms with one common attribute: The information these data contain does not follow a prescribed *structure* that can be systematically described and analyzed by executing formal queries against it. What commonly comes to mind when thinking of unstructured data are e-mails, MS Word and other user-created documents, voice messages, and so on.

The technical process by which data mining is carried out is often complex. While a full description of the complexities of the data-mining process is beyond the scope of this book, this chapter will focus on the ways in which the forensic specialist can use data mining to maximize the benefit to an investigation. The chapter also addresses, with several illustrative examples, how a range of data analysis techniques can assist the investigative team.

PLANNING

The bulk of this chapter is concerned with detailing the processes of acquiring and analyzing structured and unstructured data, respectively. However, before the efforts of data acquisition and analysis get under way, forensic technologists collaborate with rest of the investigative team to plan the data-mining work stream for the investigation.

Regardless of the types of data expected to be analyzed, the planning phase commonly involves collaborating with attorneys, forensic accountants, and the client's[1] business and IT personnel to address both the demand side of the investigation and the supply available to meet that demand. In other words, the forensic technology team needs to understand the investigation's scope and its objectives, leveraging that knowledge to develop a preliminary list of analyses to perform, at the same time working with the target company's finance and technology personnel to understand the availability of data that would be needed to meet the demand. These two sides of the planning process are discussed next, as well as a discussion of the different methods of acquiring data.

Develop Preliminary List of Analyses

Given the massive volumes and widely diverse types of data that are available throughout any enterprise, a clear understanding of the investigation is useful in guiding forensic technology practitioners to the data that may be relevant to the investigation. Thorough discussions covering the investigation's background, its known facts, and immediately known objectives should take place among all members of the investigative team.[2]

For example, as the team is embarking on an investigation of alleged FCPA violations, it is useful to understand the background and the events that led to the events being investigated; the territory(ies) where the alleged acts took place; the contracts and products involved; the divisions affected and their common contracting procedures, processes, and controls; the roles and positions of the individuals involved; and the timeframes and changes that took place over time.

Understanding the investigation's scope and its objectives naturally leads to the development of potential questions that will need to be addressed in the course of the investigation. Identifying what information is required to answer these questions leads to an identification of the types of data that should be collected and the analyses that should be performed.

The cooperation of the target company's business and technology personnel can be invaluable in determining and understanding the process flows and the system structure to aid in drafting the preliminary list of analyses that could be completed. Circumstances may exist, however, in which the client's personnel are unable or reluctant to help or they find themselves suspected of being complicit in the suspected fraud. In such circumstances, the forensic technologist will need to seek out other

[1] Throughout, these concepts applicable to *client* or *client systems* also apply to work done on an adversary or investigative target's systems. It is of critical importance that counsel be involved in working out the protocols to be followed when such access and cooperation is afforded, since system integrity, degree of access, and the likely inability to continuously reaccess systems, premises, and personnel are all potential issues and constraints that need to be addressed definitively.

[2] It should be noted that the nature of investigations is highly fluid; the needs, and thus data requirements, would likely change over time. Yet, this does not diminish the need to have thorough planning completed up front using any and all facts available at hand at that time.

ways to obtain this information. A helpful source in this regard is often the systems documentation itself. Alternatively, inspection of the systems might also yield valuable information, particularly if the analyst is familiar with them.

Understand Availability of Data

Once the investigative team has defined what analyses would be of value and thus what types of data they should attempt to obtain, given the objectives and the nature of the investigation, work needs to be done to outline the availability of these data at the target company. In reality, investigators frequently work on addressing data availability and drafting a preliminary list of analyses simultaneously, going through several iterations and refinements, as new facts gained around data availability may affect the earlier decisions made with respect to potential analyses and vice versa. Updating the list of analyses may also point the investigators to a different type of data they may target at the client.

Understanding Available Data Sources

An important first step in preserving and collecting data is to identify all of the different locations within a company's environment where the data could exist. Relevant data can exist on network servers, user laptops and workstations, backup media, e-mail archives, decommissioned servers, web servers, and so on. A data map is a useful tool in understanding the sources of potentially relevant data. Beyond just the locations of the various data, data maps also contain information about the nature of the data stored (date ranges, files types, user access, and so forth), the associated retention policies, the system owner, and other information critical to determining the value of the data to the investigation. The data map can also provide a framework and prioritization schema for the data collection plan.

If a current data map is not available, the analyst must determine manually where and what (and for how long) information is maintained. Because of the complexities of today's information system environments, even establishing the universe of systems in place and their ownership, as well as identifying subject matter experts for each, may be a challenge. Some companies maintain asset tracking systems to control accountability over systems and databases and records retention schedules to delineate the timeframe for which various record types should be maintained. While these systems may not be current or well maintained, even an incomplete asset tracking system often provides an effective starting point. The analyst should supplement any review of asset tracking information with interviews of knowledgeable people, a review of systems documentation from the company's IT staff, and a walk-through of the data center(s). During this process, one must locate as many relevant systems and data storage locations as possible, including systems that physically reside at employees' homes and systems that the company has recently moved to surplus or transferred to other employees. Backup media should also be included in this effort.

In their search for relevant data, forensic specialists should not focus exclusively on digital sources. Paper records can be scanned and converted into usable files with optical character recognition tools or manual data entry. For example, the paper forms describing a bank's customer businesses, their activities, transaction types, and the countries customers do business with (that is, KYCs—"know your

customer") could be scanned and parsed. These data become very helpful when they are used to augment the results of a transactional data search that identifies potentially suspicious wires sent to high-risk countries.

Defining Data Sets to Target for Acquisition

The effort of identifying target systems to collect data from should not be viewed exclusively as a technology exercise. The investigative team, composed of technical and accounting or business personnel, should gain sufficient understanding of the key business processes relevant to the investigation. Understanding business processes, related cycles, and controls is instrumental to properly mapping them to associated data flows and subsequently the target systems that house data sets of interest. Also, such business knowledge is essential when the collected data are to be interpreted, analyzed, and reported upon.

Data can come from many different sources within an organization, and while financial reporting systems are frequently the most commonly thought of data sources, less obvious sources may exist from which supplementary information can be gathered. The integration of data from several sources can be one of the most productive investigative methods for the forensic analyst. While fraudsters can alter data in one or several of the enterprise's systems, the complex relationships and interdependencies that naturally exist between data in numerous systems make it almost impossible to cover all traces of their activity throughout the enterprise. The forensic investigator's ability to cross-check various data sources against common key fields and to identify potential inconsistencies between sources can be a very valuable investigative technique.

This discussion is especially true, given massive data proliferation and data redundancy in today's companies and their numerous operational and reporting systems. Depending on the situation, investigators may find that targeting what appear to be the same data from several systems may help to triangulate the information obtained and thereby ascertain the root cause(s) of any differences. While some of the variances are easily explained by legitimate reasons (for example, a top-side accrual that explains why the reporting system's summary line item varies from the sum of details obtained from the transactional system), others may lead to the discovery of attempts to conceal certain transactions or modifications made to systems' data to cover fraudulent activity.

In deciding which data set (or group of data sets) to acquire, a compromise needs to be reached as to the degree of effort the client's personnel expends to extract the data (especially if several systems are available for a given data set) and the degree of effort the forensic technologist expends to prepare the extract for analysis. For example, the client may be able to provide standard reports that, with very little effort, can be made available in the form of text files. As a general rule, however, the forensic technologist prefers data to be in their native form whenever possible, avoiding any transformations, aggregations, or application of unknown filters and business rules that could have been applied in generating reports from that raw data.

Once the target data sets and the systems that house them are identified, the analyst should work with the system administrators to obtain a more in-depth understanding of how each system functions, its inputs from upstream systems, and its outputs downstream. In today's complex system environments, the same type of

data may be present in numerous systems, and care should be taken to obtain data from the most suitable source(s). Companies frequently rely on numerous reporting and analytical systems that consume data from their operational systems, aggregating data from multiple sources and potentially modifying them to fill a specific business need.

Understanding nuances of these transformations will help analysts to focus on the true systems of records or, where needed, obtain several instances of what may be seemingly the same data set from different points in these data's life cycle. For example, the analyst may decide to obtain transactional accounts receivable (A/R) data from the billing system for the purposes of detailed analytics as well as a summarized version of the A/R (likely including top-side adjustments) from the reporting system to enable reconciliation to the company's published financial statements.

When assessing data availability and, in particular, faced with the initial conclusion that a needed data set is not available, the investigative team should meet with appropriate IT personnel to confirm that it has searched all potentially relevant sources. Especially with multinational companies, the team should not assume that transaction processing is maintained at the location where the transactions occur. Such transaction processing or other elements of the process may have been outsourced or may be located at a central service center. For example, the data required for an operation in Pittsburgh may actually reside at a shared services center in India. The team should document in writing the information it is requesting, speak to IT and finance personnel, and ask probing questions so that information is correct and complete the first time around. In addition to live data, backup media (which may be stored by the client itself or at a vendor) may be included in considering data availability.

Considering Data Availability Challenges

The existence of data does not guarantee that they will be readily available to the forensic specialist. There may be technical, organizational, or legal barriers that potentially prevent the forensic accounting investigator from gaining access to those data. For example, in many investigations, forensic accounting investigators find that the organization's archiving system restricts access to data they need, particularly historical data. Depending on the format and media to which data have been archived, the forensic accounting team may find that the cost of restoring the archived data is prohibitive.

Time dimension and coverage should always be considered and documented when making a conclusion on the availability of a certain targeted data set. Many organizations archive only the information they are required by law to keep. Information on historical transactions may be available only in summary or overview form.

The client's security policy concerning access to sensitive information can become another limitation with regard to making data available. While such policies may not ultimately prevent the forensic accounting investigator from accessing relevant data, it needs to be considered, particularly when the project is subject to time or other constraints.

Lastly, the potential for legal restrictions governing access to the data can also prevent or slow down investigators' access to identified data of interest. Data

protection legislation is in place in many parts of the world today and being considered in others. Forensic technologists and others who are asked to investigate or evaluate such data should familiarize themselves with the relevant legislation, which may be complex. Also, while the team might legally be able to obtain and access certain information within a particular region or country, restrictions may exist on transporting that information beyond country borders. Solutions can often be found that comply with the requirements of the legal environment yet meet the investigation's needs. As each country or jurisdiction may have laws that protect privacy and even dictate whether computerized files can be removed from the premises or out of the country, a good practice is to always seek appropriate legal advice before attempting to acquire any personal data.

METHODS OF DATA ACQUISITION

Collection and preservation of electronic data is based on one important guiding principle (with all deference to Hippocrates): "First, do no harm." Investigators need to realize that the mere act of copying electronic data or booting up a computer that may contain relevant evidence on a case could compromise the data.

Numerous risks must be considered when making decisions pertaining to preservation of data. For example, the companies' internal IT personnel or their IT consultants are often asked to simply copy data. However, that approach may result in changes to file metadata and system metadata, which can present challenges to the integrity of evidence in court. It is critical that the preservation process is repeatable and defensible. The team that is charged with preserving the data needs to create comprehensive chain of custody for each individual piece of media and maintain this chain of custody throughout an investigation.

With this in mind, there are two primary methods of collecting electronic data: creating a forensic image of the target hard drive or creating a logical copy of the data. Each of these methods is described next. Qualified experts should perform the task of capturing either a logical or physical copy of media, because this process can inadvertently alter data, particularly on volatile systems such as personal computers. For this reason, one must use proper procedures, such as a write-blocking device that prevents alterations of data on the hard drive.

- *Forensic image.* A forensic image is a physical, bit-for-bit copy of a hard drive. A forensic image includes active files (those the end user can see through the operating system), deleted but recoverable files, and information stored in unallocated and slack space. Forensic imaging also captures vast amounts of additional useful information, such as metadata, and useful fragments of files that can be used to reconstruct items such as Internet surfing histories as well as instant messenger communications.
- *Logical copy.* A logical copy of media captures only the content visible to the device's operating system, also known as *active files.* A logical copy of a hard drive will not include files marked for deletion even if the file still resides in the unallocated space.

As it relates specifically to structured data, there are two primary ways in which the data may be preserved and acquired in an investigation. Either the servers on which the relevant data reside can be imaged using forensically sound techniques, or client IT personnel can extract a logical copy of the relevant data. The choice of method can depend on a number of factors such as the dynamic nature of the underlying data and the ability to assert completeness of the data if a logical copy is extracted by client IT personnel.

In conclusion, it is worth emphasizing again that, during the planning phase, the forensic technologist should be working side by side with the forensic accountants to continuously relate the objectives of the investigation and its intended analyses with the observations on the available data that could be relevant to the collection of evidence. Close coordination between the forensic accountant and the forensic technologist during these initial stages of the investigation, before the extraction of data from the organization's systems, can save all parties valuable time and effort and, more importantly, greatly improve the effectiveness of subsequent investigation phases.

STRUCTURED DATA ANALYSIS

The process of using structured data for a forensic accounting investigation can be divided into four stages: preservation and collection; assessment; preparation; and analysis and reporting.

The *data collection* stage is the process of requesting and accessing data to be used in the analysis. *Assessment* involves verifying the quality of acquired data, its accuracy and completeness. During the *preparation* stage, data sets acquired are normalized, and multiple data sets acquired from disparate sources may be harmonized to allow creation of a single data repository for any subsequent analysis. In the *analysis and reporting* stage, data analytics tools are applied to derive the facts and conclusions that are of interest for the investigation. Besides the actual results, a detailed summary of all the steps taken and conclusions reached in the investigation of a case is prepared.

The Data Collection Stage

This stage must be completed efficiently and each step taken with caution as the successful completion of the remaining stages of the process entirely depends on how well the first stage is performed. In developing the data request, the analyst should gain an understanding of the relevant business processes and related systems to ensure the data being acquired will meet the objectives of the data mining.

When collecting structured data from client systems, the analyst should articulate the request in as much detail as possible. The request should include written instructions for specific tables, fields, time periods, and control totals used for reconciliation purposes. The request should also specify the preferred method to extract the data from source systems and preferred media types for the data delivery. Measures should be taken to protect sensitive and confidential data: It should be encrypted, providing the key only to the requestor. The method of transmission should also be considered to protect confidential and sensitive information.

Upon receipt, all incoming data sets should be logged to create an inventory of information received and to track what remains outstanding. The inventory follows the format of the data request and should include at least the following information for each receipt: date received, the sender, the recipient, shipment method with tracking information included, media (for example, DVD, portable hard drive), description of the file, and file name(s).

Inventorying the data will prove critical to maintaining an audit trail and to managing the large volume of data often received in complex matters. The inventory is also a helpful project management tool to give the team visibility into its progress of receiving data.

The Assessment Stage

During this stage, the acquired data are loaded into an appropriate database environment and tested to assert its quality, accuracy, and completeness. It is critical that this stage is not taken lightly and is completed while applying a great deal of care and diligence. Faulty analysis often occurs when one rushes to obtain answers from the data before understanding them well and ensuring their completeness and accuracy. While teams often work under pressure to produce answers soon after they receive data, faulty answers can jeopardize the success of the investigation.

Platform Selection The choice of a proper analytical platform is driven by several factors such as data set size, its native format, and the types of analyses expected to be performed on the data.

While some simple smaller data sets can be analyzed using common spreadsheet software (for example, MS Excel), use of spreadsheets is generally not advisable because spreadsheet programs lack some critical controls and features present in more powerful database software packages. Relational databases should be deployed to leverage their feature sets including comprehensive security and access restriction mechanisms, ability to establish and maintain referential integrity, powerful querying capabilities, ability to link numerous data sets, and so forth.

Among the relational database packages, those commonly used include MS Access (for smaller data sets), MS SQL Server, and Oracle. When properly configured and supported by adequate hardware, both MS SQL Server and Oracle can efficiently handle some of the largest data sets, running very complex advanced analytics.

In some cases, though, a more specialized software package may need to be deployed. For example, software packages such as SAS or SPSS are commonly used for advanced statistical analyses. Another example is use of software geared toward detecting a specific type of fraud or financial crime. There are a number of commercially available software packages that have analytical engines and additional functionality (for example, identifying hidden relationships between individuals or entities) aimed at detecting money laundering activities. Other packages emphasize their enhanced fuzzy matching capabilities and powerful searches against hotlists, helpful in conducting FCPA investigations. Lastly, in addition to their specialized analytical engines, some packages offer comprehensive case management features that teams on larger or more complex cases may find to be of great value.

Data Loading Target data sets are now loaded into the selected data analysis tool. Depending on the format of the received data (for example, native database dump, flat text files, spreadsheets, and so forth), data transformation may need to take place for it to successfully load the data. However, the transformations should be limited to formats and data types, not content of data, thereby ensuring the integrity of the original data.

All data transformations should be documented, and a map of tables created in the data analysis tool to the original files received should be added to the data inventory. The loaded tables should remain intact throughout the duration of the investigation. To the extent it is possible and practical, account access restrictions can be used to ensure these data remain intact.

In many cases, the data analysis tool's built-in data import functionality is sufficient to import received data. Sometimes, however, it is necessary to apply special tools and methods to convert and import data received in some proprietary formats or in a nontabular form (for example, a report).[3] For example, one can transform report files into a table format using third-party software products such as Monarch or using custom-generated scripts. One can extract data within certain PDF files using custom software applications available for purchase.

Data Quality and Completeness To most effectively analyze the data and produce reliable results, one must gain sufficient comfort over the quality of received data and their completeness. The initial completeness tests can be of a purely mechanical nature and include confirming that the control totals and row count currently residing on the data analysis platform are the same ones that the team received from the client.

With respect to data quality, analysts should determine whether the actual data and data model conform to the knowledge gained about the data earlier in the process, including record layouts, data dictionaries, and interviews with IT and business personnel. The team must document deviations from the expected data model into an issue log that a team member will track for resolution.

Data quality assessment can be simplified by using commercially available data profiling tools (for example, Informatica). The tool can be configured to address both data validity (that is, nulls, allowed ranges, data formats) and data accuracy (that is, a more comprehensive analysis testing conformance of data to the stated business rules and table or field interrelationships). This testing step may include attempting to establish referential integrity between the elements of the data sets based on the business rules provided and identifying exceptions (for example, orphan payments with no matching vendor records).

Once analysts have investigated issues within individual data sets and between data sets with known relationships, they document in an issues log the inconsistencies and work with the client to follow up. As analysts resolve problems with the data,

[3] Data originally housed on mainframes may be produced in non-ASCII character sets, EBCDIC in particular. These data can be converted to ASCII before being loaded (for example, using MKS Toolkit) or fully loaded as a binary file and then converted with a custom script. In some cases, third-party vendor assistance may be sought to convert data provided in a format that cannot be easily read. Many vendors specialize in the conversion of data from legacy systems.

they should make note of the resolution in the issues log. Performing these steps well provides the team with a deep education into the particularities of the data, which will drive more efficient and effective analysis later in the investigation.

After investigating and resolving the issues within the data, analysts must gain comfort over the completeness of received data. In many instances, in particular dealing with financial data such as general ledger or inventory data, it is highly advisable to reconcile the data to financial reports, and ultimately, to audited financial statements.

For example, one should be able to trace the contents of an accounts receivable subledger system up to the comparable line item(s) in a public company's financial statements. Dealing with large complex entities, this reconciliation may become a very involved process, as the team may have received the data from numerous systems and, to be able to reconcile against consolidated financials, the data would need to be consolidated. Companies also frequently book adjustments to their subledger amounts before posting. The adjustments may be significant and, unless obtained and taken into account, present a significant obstacle to successful reconciliation.

Other methods of gaining comfort over data completeness include comparing independently calculated statistics on the data obtained against management reports or comparing summaries of several data sets received or obtained from other sources (for example, company press releases or bank statements obtained from the bank), observing whether there is a relationship that would be expected given the nature of these data sets (for example, comparing movements of inventory to sales records, comparing bank account transactions representing wires to the download from the bank wire processing system). Such triangulation, while not as precise as reconciliation against financial statements, can be used either independently or in conjunction with other methods to strengthen the level of reliance on an otherwise imperfect comparison.

Depending on the circumstances of the data and related problems, the analyst will reconcile the data to summaries either with no variance or within a level of tolerable error. Without confirming the data's quality and completeness, the parties cannot rely on any analysis of the data and its outcomes. Analysts should continue to verify the data's integrity and comprehensiveness at various stages of data analysis as new facts about data attributes may become known.

The Preparation Stage

As described in the previous section, the received data are first loaded into a data analysis platform with a minimal amount of modifications, to most accurately reflect the format and content of the data received. However, while doing that preserves integrity of received data, the imported tables may not be most suitable for analysis without completing some data preparation steps. It is imperative that amendments made at this stage not affect the accuracy of the information.

All modifications and refinements made to the data at this stage should be documented, explaining the rationale for the changes and steps taken, as well as retaining any executed scripts. The log may be needed at a later date to prove the integrity of the analyzed data and its relation to the information extracted directly from the organization's systems. Analysts should not modify the original data, but

instead place the modified values into additional data columns or tables, as necessary, using a consistent naming convention for the column and table names.

The following are three examples of commonly applied procedures, data cleaning, deduplication, and consolidation, to illustrate how preparing the data can assist in the data-mining process.

Data Cleaning This process involves a host of procedures aimed at standardizing the data to make them suitable for use with the analysis tool selected as most appropriate for the data analysis exercise. Data cleaning can also involve the standardizing of common abbreviations within a data set and removing extraneous information. These steps make useful information available to the forensic accounting investigator.

Examples of factors that necessitate cleaning and harmonization of data include formatting issues (for example, dates presented as coded text), inconsistencies between similarly purposed data sets received from several systems of the same company (for example, SAP and Oracle), different units of measure or currency for data received from international territories of the same client (for example, "02052010" representing February 05 for the U.S. data set and May 02 for the European one), and coded values that need to be disaggregated for the purposes of the analysis (for example, "01123" representing invoice number 123 issued by company number 01).

The information and documentation gathered earlier about the systems collected can now be used to identify the types of data stored in various tables in fields, so that common elements from disparate systems may be mapped together.

Data Deduplication One of the problems analysts may encounter is that multiple copies of various data sets may be recovered as part of the investigative process. To ensure the accuracy of the results, the elimination of duplicates (deduplication, or deduping) in the recovered data sets is often the first order of business after the data have been acquired and the documentation has been completed. One might suspect that deduplication would be a straightforward process; several variations of the process, however, need to be considered before work can begin.

Most importantly, the analyst must decide what qualifies as a duplicate. In its simplest form, deduplication is completed by defining the set of fields, also known as a *key,* which distinguishes each record as a unique object (for example, a combination of company code and invoice number), and then by identifying and consolidating records with the same key.

At times, however, this process is complicated by the same business object (for example, a single invoice) being presented differently in legacy versus current systems. As such, there could be some hidden duplicates that don't appear as such based strictly on the key values. In these cases, knowledge of the systems gained in the earlier phases of the investigation is used to build some more complex duplicate identification rules. Sometimes, duplicates are not excluded completely and are dealt with as a result of completeness assessment exceptions or once some analysis results are reviewed later in the investigation.

As duplicates are eliminated, care should be taken when making decisions as to which records survive. While two or more seemingly duplicate records may have the same key values, the values of their other fields may vary. For example, some of the other fields may have been populated or corrected in the later instances of the data sets but remained unchanged or blank in the earlier archived versions. Sometimes,

entire records cannot be chosen, and these decisions are made on a field-by-field basis, whereas values for different fields are chosen from different records. It is also possible to retain more than one value for a given field pending further analysis.

The processes of deduplication and completeness assessment are frequently done iteratively as completeness issues identified may point to yet another set of duplicates in the data not dealt with earlier.

Data Consolidation Many companies have multiple ledgers and operational and financial systems because of mergers, acquisitions, or international operations. Sometimes companies phase in new accounting or ERP applications so that not all divisions will have their accounting or other applications on the same platform. These situations make it difficult to view the data in a consolidated or consistent manner across the enterprise. While not always possible, data obtained from several similarly purposed systems (for example, several different billing systems) can be transformed and consolidated into a single analysis-ready data set. In other cases, this may not be possible or practical; analysts would continue to work with several systems but would have to consolidate all obtained results.

Systems may present information at different levels of details (for example, one system reflecting each individual line item on an invoice while another only shows the total amounts). Furthermore, some systems may contain data attributes that others do not (for example, one system showing the counterparty bank for a wire transaction while another presents only the country). The consolidated database schema has to account for these differences. Yet again, a decision may be made not to create a comprehensive database but rather to continue working with individual data sets independently, consolidating the results later.

The consolidated data set should have addressed the differences observed between the data initially housed in different systems or databases. It may need to be further enhanced to ease analysis and make it more reliable. Examples of supplementation include parsing of columns containing multiple pieces of information (for example, one field containing city, state, and zip code; or one field containing both a department code and an account number) or calculating various values within a data row (for example, adding freight, tax, and product costs to get a total invoice price).

The Analysis and Reporting Stage

The analysis of structured data occurs throughout the investigation process from identifying suspicious transactions for further investigation to quantifying the extent of the fraud. Because case strategy evolves as more evidence comes to light, the team must stay in communication to advance and inform the case strategy. The evolution of the strategy will affect the types and substance of the data analysis to be performed.

The actual steps performed at this stage vary greatly from one investigation to another, driven by the nature of the allegations. A commonality across investigations, though, is to ensure sufficient documentation to support the integrity of the analysis. All business rules, simplifying assumptions made, directions taken, and the actual scripts must be documented to enable an independent re-execution of the analysis (obtaining the same results) if so requested.

Data Analysis in Action: Examples The forensic teams can use data analysis techniques in many situations. Whether conducting proactive procedures as part of an internal or external audit or performing reactive procedures to resolve allegations, the teams will likely find that data-mining techniques are efficient and valuable. The following examples touch on several areas in which data analysis has proven to be of great value and, at times, the cornerstone of the investigative work. The types of investigations examined include asset misappropriation, financial statement fraud, money laundering, anticorruption or FCPA violations, and Ponzi schemes.

Asset Misappropriation The procure-to-pay cycle is an area in which data analysis techniques have been historically used most often to detect fraud and other irregularities as well as to test the adequacy of controls in place. This cycle's susceptibility to asset misappropriation fraud as well as high volumes of data supporting this business cycle make it a natural area in which deploying data analysis tools can serve as an effective detection mechanism.

Examining payment details and matching those against the employee master may reveal payments of large sums to vendors who are also employees. In a recently conducted test (see Exhibit 17.1), analysts identified such payment in the amount of $122,125. Using more advanced matching techniques, identifying similar exceptions could be based on partially matched names and the same or similar addresses:

EXHIBIT 17.1

Address	ID	SSN	Payee	Telephone Number
617 SHERIDAN AVE NEW ORLEANS LOUISIANA 70265	70328	390627191	DAVIS, SANDY J.	256-555-1872
617 SHERIDAN AVE NEW ORLEANS LOUISIANA 70265	70198	625480632	E & S Transportation	256-555-1872

Tests aimed at detecting duplicate vouchers may identify such double-billings issued by different branches or locations of the same vendor. While the vendor IDs on the two vouchers may be different, the same amounts, proximity of the billing dates, and closely matched names point to a potential erroneous or fraudulent billing. (See Exhibit 17.2.)

Exhibit 17.3 offers an example of payments made to a particular vendor. The invoice numbers from that vendor are in sequential order without gaps—as noted by sorting the invoice register by vendor and by invoice number. Further investigation revealed that these invoices were from a vendor established by the purchasing

EXHIBIT 17.2

Vendor ID	Vendor Name	Invoice Date	Invoice Number	Amount
6147	Vendor One	3/26/09	103-7519143	$25,740
6275	Vendor 1	3/27/09	103-7523427	$25,740

EXHIBIT 17.3

Ck #	Ck Amt	Inv #	Inv Date	Inv Amt	Ordered	Rec'd	App'd
2065	53,686.60	317	11/02/2009	30,905.60	R.M.	J.D.	R.M.
2065	53,686.60	318	11/22/2009	2,101.00	R.M.	J.D.	R.M.
2065	53,686.60	319	11/22/2009	20,680.00	R.M.	J.D.	R.M.
2478	160,668.20	320	01/17/2009	25,124.00	R.M.	J.D.	R.M.
2478	160,668.20	321	01/17/2010	51,177.50	R.M.	J.D.	R.M.
2478	160,668.20	322	01/17/2010	84,366.70	R.M.	J.D.	R.M.

manager, who was the focus of the whistle-blower allegations. The purchasing manager was behind the scheme and had not disclosed any conflict of interest. Note as well that the employee ordering the goods, R.M., also approves the invoice for payment.

Financial Statement Fraud Detecting fraud in financial statement preparation can also benefit from deploying data-mining techniques. General ledger data analytics help to effectively process very large numbers of journal entries and identify a subset of those that warrant a closer review by financial teams, as they contain potential fraud red flags.

Exhibit 17.4 presents results of analysis aimed to identify reversing entries. The sample listing provides manual journal entries posting revenue credits with P&L impact greater than $5,000,000 that have been subsequently reversed after the books are closed. This analysis addresses the potential of management's override of controls, specifically by posting a journal entry that may materially affect the financials and subsequently reversing amounts in an ensuing period or quarter.

Another example of journal entry analysis identifies backdated entries. Such transactions may reflect management's override of controls, specifically through backdating entries with a material impact on the financials. While closing entries and adjustments are commonly posted in the month following the reporting period, the following test was performed to identify journal entries that were entered more than one period after their posting date (something the company stated should not happen in the ordinary course of business. See Exhibit 17.5).

Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) Outside of the financial reporting space, financial institutions rely greatly on data analysis to identify

EXHIBIT 17.4

Original/ Reversal	JE No	Rev Cr	Rev Dr	JE Desc	JE Post Date
O	951011	5,766,010	0	ZZ FEE RECE ZZ	12/21/2009
R	984012	0	5,766,010	ZZ RECLASS # ZZ	1/14/2010
O	951487	6,745,100	0	ZZ HOLLAND I ZZ	12/23/2009
R	983832	0	6,745,100	ZZ REVERSAL ZZ	1/10/2010

EXHIBIT 17.5

Journal ID	Source	Period Num	Entry Month	Entry Year	PL Impact
64883774	GLD	6	8	2009	(275,025.80)
64883773	GLD	6	8	2009	10,331,966.00

potential BSA or AML violations. Data analytics are at the core of monitoring transactions on their customers' accounts to identify and investigate potentially suspicious activities.

A common example of deploying data analytics to detect potential money laundering is *cash structuring* analysis. Federal law requires that financial institutions report cash transactions in amounts at or above $10,000 through the filing of a Currency Transaction Report (CTR). In an effort to circumvent this requirement, a tactic known as *cash structuring* may be employed, which splits large cash transactions over multiple smaller transactions, all of which are under the CTR requirement threshold of $10,000. Transactional monitoring techniques identify such suspicious patterns of activity. In Exhibit 17.6, customer J. Smith is conducting multiple cash transactions, in the month of March 2009, that are below the CTR requirement. This report would be used by the investigative team to further research those activities and determine whether the smaller amounts are reflective of money laundering and CTR avoidance.

Identifying wire transfers to high-risk countries is of utmost importance to financial institutions because of their potential connection with terrorist funding, money laundering, and fraud. In practice, identifying the source and destination of wires can be an arduous effort. Exhibit 17.7 shows two separate wires, each of which is for $1,000,000. One of these wires is of much more interest than the other. The first wire is a domestic wire to a recipient in Peachtree, Georgia, whereas the second wire is to a recipient in Tbilisi, the capital city of the country of Georgia. Since Georgia has been identified as a high-risk country, high dollar transactions associated with it could be investigated by the financial institution. To the contrary, Peachtree, Georgia, is not of any special importance and manually reviewing wire transactions associated with it would place an unnecessary burden on the institution. Advanced analytical models can be used using powerful free text searches to effectively identify high-risk wires and reduce false positives (similar to this first record).

Anticorruption and the Foreign Corrupt Practices Act (FCPA) Data analysis is an effective tool to monitor compliance with and to conduct investigations of alleged

EXHIBIT 17.6

Transaction Date	Customer Name	Account Num	Type of Transaction	Amount
3/6/2009	J. Smith	xxxxxx7458	Branch Cash Deposit	$9,500.00
3/10/2009	J. Smith	xxxxxx7458	Branch Cash Deposit	$8,550.00
3/11/2009	J. Smith	xxxxxx7458	ATM Cash Deposit	$9,000.00
3/14/2009	J. Smith	xxxxxx7458	Branch Cash Deposit	$9,900.00

EXHIBIT 17.7

Transaction Date	Customer Name	Account Number	Wire Amount	Wire Description
2/25/2010	M. Smith	xxxxxx6723	$1,000,000.00	1374 First St., Peachtree, Georgia
2/25/2010	T. Detter	xxxxxx8738	$1,000,000.00	Alexander Durmra St. N5, Tbilisi, Georgia

EXHIBIT 17.8

Agent Name	Time Period	Sales Quantity	Sales Amount	Commission Payments	Commission as a % of Sales
Joe Smith	Jan. 2009	15	$20,000	$2,000	10%
Joe Smith	Feb. 2009	30	$40,000	$8,200	21%
Joe Smith	Mar. 2009	8	$30,000	$3,000	10%
Joe Smith	Apr. 2009	5	$15,000	$1,500	10%

violations of the FCPA. The driver here is the same as in the previously described areas: numerous disparate systems and large volumes of transactions subject to analysis.

In FCPA cases, when facilitation payments are made by third-party agents acting on behalf of a company, analyzing commission payments as a percent of sales can be very useful. In Exhibit 17.8, from a recent FCPA investigation, sales agent Joe Smith receives commissions for any sales he makes. In general, his contractual commission percentage is 10 percent of total sales, but in February 2009, the commission percentage increases to 21 percent. By analyzing commissions and sales data, such irregularities were identified and investigated.

By analyzing a company's payment register, foreign payments made to entities in countries that rank higher on Transparency International's Corruption Perception Index (CPI) can be identified. This index ranks countries in terms of the degree to which corruption is perceived to exist among their public officials and politicians. (See Exhibit 17.9.)

It is common for companies to have controls requiring approvals of all payments over a certain threshold. To circumvent this control, facilitation payments can

EXHIBIT 17.9

Vendor ID	Vendor Name	Vendor Country	Vendor Bank Country	Number of Payments	Amount of Payments
123	ABC Corp.	United Kingdom	Russia	10	$904,748.66
456	XYZ Inc.	Angola	Angola	2	$156,980.00

EXHIBIT 17.10

Employee ID	Employee Name	Payment Date	Payment Amount
3654	Brad Jones	1/3/2009	$6,000
3654	Brad Jones	1/5/2009	$3,000
3654	Brad Jones	1/8/2009	$4,000
3654	Brad Jones	1/8/2009	$2,000

be made in smaller increments, which can be detected by completing a threshold aggregation analysis. The test in Exhibit 17.10 detects multiple payments which, when aggregated, exceed a threshold. An example of this would be an employee being paid multiple times through the T&E system with false claims and using the money for facilitation payments. In the following example, none of the individual payments made to employee Brad Jones exceed the $10,000 threshold that would require managerial approval. However, in aggregate, these payments would have exceeded the threshold.

Ponzi Schemes In the wake of recently uncovered Ponzi schemes, forensic teams have applied data-mining techniques to aid with the discovery of the facts, recreation of the events that led to the scheme collapse, and tracing of the sources and uses of funds.

As financial statements and underlying journal entries often cannot be relied upon in an entity running a Ponzi scheme, the forensics team will rely on cash activity to base its analysis. In one recent case (see Exhibit 17.11), certain bank statements were forged by employees to present a picture of financial health to potential investors. Exhibit 17.11 is an example of a bank statement analysis that was performed to measure average activity from month to month for a particular bank

EXHIBIT 17.11

Statement Start Date	Statement End Date	Total Credits	Total Debits	Reviewer Comments
1/1/2002	1/31/2002	$7,790,045.13	$4,922,144.00	
2/1/2002	2/28/2002	$6,730,817.53	$5,394,870.52	
3/1/2002	3/31/2002	$8,601,779.58	$10,794,338.45	
4/1/2002	4/30/2002	$8,497,766.81	$7,507,965.14	
5/1/2002	5/31/2002	$1,157,236.02	$1,157,238.94	
6/1/2002	6/30/2002	$3,277,666.87	$6,267,400.18	
7/1/2002	7/31/2002	$22,130,232.82	$18,529,018.92	Requires further investigation
8/1/2002	8/31/2002	$3,982,554.61	$6,597,218.21	
9/1/2002	9/30/2002	$2,089,719.40	$2,089,728.81	
10/1/2002	10/31/2002	$4,437,343.55	$4,437,472.33	
11/1/2002	11/30/2002	$7,711,257.92	$5,094,159.33	
12/1/2002	12/31/2002	$26,799,145.80	$29,416,310.60	Requires further investigation

EXHIBIT 17.12 Transaction Detail

Bank Account	Clear Date	Payer	Payee	In Amount	Out Amount
1	2/8/2005	*Unknown*	ABC	$25,000.00	
2	2/8/2005	DEF	*Unknown*		$25,000.00
1	2/10/2005	*Unknown*	ABC	$90,000.00	
3	2/10/2005	XYZ	*Unknown*		$90,000.00
2	2/12/2005	*Unknown*	DEF	$100,000.00	
3	2/12/2005	XYZ	*Unknown*		$100,000.00

account. The analysis helped identify statements from July 2002 and December 2002 that were likely forged based on the unusually higher volume of debits and credits.

With the forensics team relying on cash activity to base its analysis, data-mining techniques were used to consolidate activity from multiple bank accounts and to present a consolidated picture of sources and uses of funds. Difficulties were encountered in two ways: harmonizing the data elements contained in bank statements when each bank presents a different level of detail in its account statements, and eliminating wire transfers between company bank accounts so as not to count the transfer of funds twice. Exhibits 17.12 and 17.13 illustrate both of these difficulties by listing the detail transactions from each account first and then a summary after deduplication second.

UNSTRUCTURED DATA

Unstructured data, while not maintained in a database or structured archive, can provide valuable information to an investigator. However, it typically requires more effort to extract and analyze. We next explore some different types of unstructured data, leading practices on the collection and preservation of such data, and various analytical techniques that may be used to extract information that may be valuable to an investigation.

Types of Unstructured Data

Unstructured data can exist in many forms and locations in an enterprise. The following details some of the more common forms of unstructured data that are often useful to an investigation.

EXHIBIT 17.13 Summary after Deduplication

Clear Date	Amount	Account 1	Account 2	Account 3	Payer	Payee
2/8/2005	$25,000.00	In	Out		DEF	ABC
2/10/2005	$90,000.00	In		Out	XYZ	ABC
2/12/2005	$100,000.00		In	Out	XYZ	DEF

User-Created Files Files such as Microsoft Word documents, Excel spreadsheets, Adobe Acrobat files, and PowerPoint presentations that have been created and saved by users of a computer system are commonly referred to as user-created files. These files are distinguished from system, application, and template files that reside on every computer or server. User-created files typically exist in a number of different places in a company's network: on the user's desktop or laptop computer, in home directories and shared folders on the company network, on external storage devices such as flash drives, attached to e-mails, and on backup tapes, to name a few.

Electronic Communications The most valuable information in an investigation is often found in the electronic communications among employees. The use of e-mail has exploded over the past decade, surpassing all other written forms of communication combined.

Many e-mail users neglect caution and discretion when they create messages. The candor engendered by e-mail's illusion of privacy can create a trail to establish intent and awareness. Consequently, investigators often find that electronic communications provide compelling evidence of the intent of the parties, a key element of white-collar crime investigations. Former deputy U.S. attorney general James Comey noted that "E-mail is a window into the mind."[4] Investigators find e-mail valuable because the author's guard may be down, thereby revealing intent, and unlike shreddable paper, destroying e-mail can prove difficult.

Most medium- to large-sized companies use network-based e-mail applications like Microsoft Exchange or Lotus Notes for e-mail communications. These applications will typically store user e-mail centrally on the network as well as allow users to replicate their e-mail boxes to their laptops or workstations. Many companies have deployed e-mail archiving systems in an attempt to provide more structure to their e-mail repositories for compliance or storage purposes. While these systems do provide a more searchable context for corporate e-mail, most are primarily storage repositories of largely unstructured data.

Smaller companies will typically deploy a web-based e-mail system such as Gmail or Yahoo Mail for their employees. With this approach, there is no central repository of e-mail for the company; user e-mails are routed through the web-based application and are sent directly to the user. It is worth noting here that web-based e-mail solutions are being evaluated by increasingly larger organizations as part of the movement toward cloud computing. Web-based mail systems and those hosted in a cloud environment present distinct challenges when considering preservation and collection of e-mail. A discussion of these challenges is beyond the scope of this chapter, but when such systems are encountered, it is advised that one seek the advice of experts in this area.

Another widely used form of communication is instant messaging (IM). In the past few years, instant messaging has become a key component of both internal and external corporate communications. Beyond just simple conversation, IM technologies also allow users to share documents, links, videos, and more. With the exception of financial institutions that are subject to more stringent data preservation requirements, most companies do not store IM transactions. Those that do store the data

[4] http://aol.businessweek.com/magazine/content/04_08/b3871100.htm.

typically do so only in unstructured form and for short periods of time. This makes collection and analysis of IM data challenging.

Computer Usage and Access Logs Depending on the form in which they are maintained, web logs, Internet logs, access logs, and so on can be classified as structured or unstructured data. Most companies do not maintain these logs in a readily analyzable form. Furthermore, many companies overwrite these logs frequently, making historical analysis difficult.

Collaborative Technologies Knowledge management and collaborative technologies such as Microsoft's Sharepoint, intranet portals, wikis, and so on can also provide a rich source of data for an investigation. These technologies allow users to post documents, create content, and conduct dialogues about various topics. While these tools provide a structured environment for knowledge sharing in an organization, the data that are compiled within them are difficult to access, compile, and analyze. Specific expertise in this area should be sought when one has a need to preserve and collect data from these sources.

Metadata Metadata, which literally means "beyond the data," are the system-generated attributes of a particular file. Metadata is not apparent when files are printed to paper or converted to an image format such as a TIFF or PDF file. When computers store information for later retrieval, the operating systems create certain data about the stored information so they can facilitate ongoing processing. These attributes can include fields such as the name and location of the file, name of the author, the name of the person who last saved the file, the date the file was created and last modified, and size of the file, and the number of revisions the file has gone through, and so on. Some programs also allow users to add their own metadata to a file, such as a document title, the subject of the file, the name of the author of the document, the name of the manager responsible for the document, and the name of the company that owns the document. Also, some programs permit a user to assign metadata to a document in order to facilitate later retrieval. This type of metadata can include assignment of the document to a particular category, inclusion of searchable keywords, or a description of the document's contents.

In addition to these types of metadata, there are other, less obvious variations that can be critical in an investigation. For example, spreadsheets and databases can contain complex mathematical formulas and links among fields, which play key roles in calculating the numbers that appear in various cells. Typically, the printed spreadsheet will show only the result of the calculation, not the formula used to calculate the result. Similarly, modern word processing documents can contain links and references to other types of electronic files such as pictures, charts, spreadsheets, and sound files. These linked files may be stored either in the same location as the main document or halfway around the world on another computer linked by a proprietary network or by the Internet. The printed document may show the content of the other files without revealing that those elements are not integral parts of the electronic document but are really borrowings from other electronic sources. The electronic document will necessarily contain the code needed to connect to the data in the linked files and may give a forensic accounting investigator pointers to additional

sources of relevant information. This in turn may lead to additional witnesses, such as the author of a linked document in a remote location.

Deleted/Slack/Unallocated Space Up to this point, our overview of the types of unstructured data has centered on active files stored on a computer system, backup tape, server, or other electronic media—that is, files that are readily accessible by a user or investigator. One of the advantages of computer forensics is that an investigator is not limited to examining active files. As most now know, when files are deleted from a computer hard drive, the files themselves are not erased; merely references to the file are removed by computer's operating system. The actual file data are typically not erased from the drive until they are overwritten by an active file. Although this unallocated space generally cannot be seen by normal operating system tools—such as Windows Explorer—it can be seen, searched, and sorted by computer forensic tools. Some data in unallocated space will be fully recoverable as if they had never been deleted. Other data may consist of file fragments that have been partially overwritten. While such data may not be fully recoverable, they may still provide clues about the computer user's activities.

Computer forensic tools can also search through the space at the end of files between the end-of-file marker and the end of the cluster in which the active file data resides. This slack space, not being used by any active file, may contain bits of data from files long ago marked for deletion from the hard drive. Forensic tools can search and find data stored in these spaces that might otherwise go undetected if drives are simply copied rather than imaged.

There are several potential limitations on the use of data discovered in slack and unallocated space. First, it may not always be possible to attribute dates accurately to such information because the normal operating system dates will not typically be available. Second, highly fragmented data found in slack or unallocated space may be hard to place in context. For this reason, drawing conclusions about the data may be difficult in some cases. Third, it may be hard to attribute data found in slack or unallocated space to a particular user, especially if the computer under investigation was used by more than one person.

Collection of Unstructured Data

Because of its volatile nature, extreme care must be taken in collecting unstructured electronic data. These data only exist as a series of electronic ones and zeros and are easily alterable, accidentally or otherwise.

It is important to recognize that the steps and methods used to collect data for investigative purposes are different from those used to archive data. Key metadata and file attributes can be altered by merely copying the data, making it difficult to later authenticate the data. For this reason, internal IT staff may not have the appropriate skills or experience necessary to gather data in an investigation. An investigator should insist on the appropriate preservation and collection of data in an investigative context even if it means bringing in a consultant to extract the relevant data from a company's network. The degree of formality may vary according to the size, stakes, and nature of the investigation, but a party that decides to invest in such a project will face a negligible incremental cost of doing it correctly and possible severe penalties for doing it incorrectly.

The following presents some additional leading practices regarding the collection of unstructured data.

Maintaining an Audit Trail One must maintain a clear audit trail and record of work performed to help with establishing evidence integrity. Investigators should document interviews with the IT staff while working to understand the IT systems. Investigators should also document each information request in writing, noting who requested what information and when it was requested. Such documentation has obvious benefits, but in the frenzied early stages of an investigation, many people shortcut careful, thorough note taking. However, such documentation will often prove critical, particularly if the evidence is called into question.

A best practice in the area of documentation includes the use of standardized forms, checklists, and procedures for each step of the collection and analysis of unstructured data, including the following:

- Data request form
- Evidence receipt form
- Evidence handling procedures and checklist
- Chain-of-custody form
- Imaging procedures and checklist
- Specific procedures and checklists for various operating systems (for example, Windows and Linux)
- Analytical procedures
- Overall computer forensic lab maintenance procedures[5]

Collecting Data from E-Mail and Instant Messengers Collecting information from electronic communications requires extensive effort because of its high volume and dispersion across various systems. Electronic information resides in a multitude of formats, and in myriad systems and information technology platforms. Use of non-corporate or unauthorized systems such as web-based e-mail imposes complexities that make collecting electronic communications, be they e-mail or instant messenger, costly. Review the need to collect such communications and to include such effort in the early case strategy to accommodate fiscal constraints.

One can choose from several levels of effort to recover electronic communications. Recovering logically active content requires the lowest level of effort. A complexity of dealing with logical files lies in the variety of e-mail and instant messenger applications (and file types) and how these applications store the communications. E-mail or instant messenger data stored in an uncommon or proprietary format often requires creation of a matching environment with the same hardware and software configuration as the original to analyze the information.

Depending on the type and configuration of the end user's e-mail or instant messaging system, the physical layer can recover vast quantities of information.

[5] Chris Davis, Aaron Philipp, and David Cowen, *Hacking Exposed: Computer Forensics* (New York: The McGraw-Hill Companies, 2005).

However, recovery of such communications can prove time consuming and costly because the recoverable content sometimes includes only a portion of the original file.[6] In this case, analysts use forensics tools beyond the original application to work with the content of such files.

Authenticating the Data Evidence authentication is complex, but analysts should document identifying aspects of the system, such as serial number and model, and capture independent data that may tie the use of the system to a particular employee. These independent corroborating systems can include asset-tracking systems, help-desk support applications, purchase order documents, and human resources records.

One should also tie the components to the device itself. For example, one should collect the serial number of the hard drive and then cross-reference the component serial numbers to information that one can find on the manufacturer's web site. Dell Computers, for example, allows anyone to enter a system serial number and see the serial numbers and specifications of the components. This will detect if someone swaps component parts such as the original hard drive. Personal computers with new hardware components should raise red flags of attempts to mask content that the original media would store.

Analysis of Unstructured Data

Analyzing unstructured data in an investigative context can be a challenging undertaking because of variety and volume of the underlying data. The objectives of the techniques highlighted next are to reduce the volume and normalize the data so that they can be analyzed in a structured and more efficient way.

Data Sorting and Filtering Although the ability to sort and filter electronically stored information is rather commonplace, it may also be essential to the project goal, especially when millions of e-mail messages or pages of file documents must be reviewed. Data sorting enables the investigator to separate the data into more manageable subsets for review and analysis. As mentioned earlier in the chapter, attributes such as date and time are examples of metadata, which, depending on the matter at hand, can be useful information to the forensic accounting investigator. For example, in a Word document, having a date accessed prior to a creation date is not possible. Examining this item of metadata may raise a red flag for the forensic accounting investigator. Some of the more common data sorts and filters include:

- *Date and Time*. In such sorting of computer data, many dates may be associated with a single document or data point. It is important to understand exactly what a particular date means before drawing conclusions about the data. For example,

[6] In most systems, deleting a file doesn't erase its content, but simply redefines the space it occupies as available for future overwriting. Thus, most storage media will contain fragments of partially overwritten but partially preserved files.

in a typical Windows environment, one may find up to five dates associated with each file: file created, last accessed, last written, deleted, entry modified. All of these dates will not necessarily be available for each file. And each date has a different meaning.

- *Owner or Author.* As previously noted, many programs either automatically insert author information or allow users to input author information into the metadata associated with files. It is important, though, to understand the limitations of reliance on author data. First, if the data are input automatically every time a document is created, then every document produced on a certain person's computer will indicate that that person is the author. But what if another person was for some reason using that computer? What if a computer initially issued to one employee was later assigned to another, without changing the default author setting? Then again, sometimes a document created by one user becomes a form for documents created by many other users. In this circumstance, the author information for all of the documents created from the form will reflect the original author of the form.
- *File Types and Extensions.* This sorting approach enables the forensic accounting investigator to segregate all of the word processing documents, spreadsheets, presentation slides, and other user-created files from system and program and other irrelevant files. Understand, however, that users can attempt to hide documents by adding false extensions to make a spreadsheet look like an executable program—or any other file type. Forensic practitioners can get around this situation by performing on the files what is called a signature analysis. Forensic tools can search for bits of code that are indicative of a particular type of file (file signature) and compare them with the file extensions used in the file name. If the code does not match the file extension, the tool can report a file signature mismatch.
- *Search Terms.* Search terms can be applied to an unstructured data set as a means of culling potentially responsive documents. This is a widely used method in e-discovery, particularly when the scope of a document production is relatively narrow and one has to remove large volumes of irrelevant documents. It is also valuable in a forensic investigation because it can enable the investigator to quickly spot issues that may be worth further exploration. Great care must be applied to how the search term filters are applied, as misapplication can cause key documents to be overlooked. Search term filtering, unlike concept searching, described further on, depends entirely on the quality of the search terms. Misspelled words, either in the search term list or in the data set, can cause documents to be missed. Similarly, it is difficult to develop search terms that will identify all abbreviations and colloquialisms that may be contained in a data set. As long as the investigator is aware of these limitations, though, search term filtering can be a good means of winnowing down the data volume.

ADVANCED DATA ANALYSIS TOOLS

In recent years, legal technology providers have attempted to use other tools to augment keyword searching and help the legal team understand large data populations more rapidly. A brief discussion of a sampling of these tools follows.

Data Visualization

Charts, graphs, and other images used to simplify the presentation of vast quantities of information have long been standard tools of the forensic accountant. But applying similar visualization tools to understand large bodies of textual information is a relatively new approach. Data visualization allows the user to explore data through a graphic interface instead of (or in addition to) the traditional word or phrase searches.

Concept Searching

Concept searching is the retrieval of documents based on common subject matter, rather than the existence of specific words. Thus, a concept search tool might recognize that a search for the word "—" should also retrieve synonyms such as "—" or "—". It automatically identifies the most significant patterns in any text and uses these compound terms to rank results based on an understanding of meaning rather than simply based on finding the required words. This is meant to be more adaptive and flexible than exact phrase or proximity searching. Also, queries can be expressed in natural language, with no need for complex query syntax associated with traditional Boolean techniques. Many legal professionals are beginning to use concept searching in an attempt to make the document review process quicker, more accurate, and more efficient than either paper review or keyword searching. Concept search tools attempt to learn the meanings of words from the documents they read and not just the presence of keywords so reviewers can focus on the most relevant documents first, instead of wasting time reviewing documents in random order.

Text Analytics Text analytics is a broad set of analytical methods that apply linguistic tools and techniques to structure or model data. These tools include pattern analysis, statistical sampling, named entity recognition (NER), bulk tagging, and coding of keywords. Using NER technology, for example, one can extract data into predefined categories: persons, locations, organizations, date ranges, and so on. Text analytics methods are particularly effective at weeding through large, unstructured, document-intensive data sets. A variety of tools exist from both larger software providers (for example, IBM, Lockheed Martin) and smaller, niche-focused companies (for example, Attensity, TEMIS).

Social Network Analysis A number of electronic discovery tools allow investigators to analyze the communications among various individuals through the grouping and sorting of e-mail and IM threads. This analysis is particularly helpful in identifying additional targets of an investigation.

Time Line Analysis Related to the date sort analysis discussed earlier, a time line analysis attempts to paint a picture of what happened using the dates and times of e-mails, log-in, file creation, and other user activities. As discussed earlier, one must be careful that the dates and times of activities are accurate and supportable through other analysis.

Computer Forensic Analysis As mentioned before, data in inactive areas of a hard drive can provide a wealth of information to an investigator. Beyond the obvious potential value in a deleted e-mail or file, forensic analysis can also shed light on user actions such as file deletions, sharing, modification, and copying, log-in dates and times, deleted Internet browser history and web page caches, and so on. Because of the fragmented nature of these data and the fact that the files no longer reside in the active portion of the hard drive, computer forensic technology is needed to view the relevant data and conduct much of the analysis.

CONCLUSION

Data mining is only one part of the forensic accounting investigation process. The investigation cannot be conducted from the computer screen alone. In fact, data mining should be thought of as a complement to, not a substitute for, the forensic accounting investigator's good judgment and experience. It cannot replace document reviews, interviews, and follow-up steps. The following are some final thoughts on the keys to successfully using data mining in an investigation:

- Understanding the techniques available to forensic technologists provides a wealth of information to review what would be otherwise unavailable or, at a minimum, much more difficult to obtain. In investigations, having more information is a key asset.
- Leveraging an existing data map (or creating one) that details the types of data available, their key attributes, and their location in the company's network is an important first step in determining which data to target for analysis.
- If possible, all potentially relevant data should be preserved at the outset of an engagement. Doing so reduces the risk of the data being compromised.
- It is critical to collect electronic data in a forensically sound way. In some cases, taking a logical copy of the data is not sufficient (as it results in changes to file and system metadata), and a forensic image of the target hard drive(s) should be created.
- An incorrect and incomplete data set may contribute to premature and incorrect conclusions. Data obtained should be checked for accuracy and completeness prior to any analysis being performed. The preparation of data and testing for accuracy and completeness often take longer to perform than the analysis itself.
- There are many data-mining tools available to the forensic technologist, but not all tools are created equal. Certain data-mining tools may not be appropriate for certain tasks. The type and sophistication of the tools used should be commensurate with the size and complexity of the investigation, as well as the type(s) of data mining to be performed.
- Some forensic accounting investigators may place too much reliance on the tool itself. Absent the needed blend of skilled technical use of the tools and sound analysis and judgment, many of the operational and financial benefits of data mining may be lost.
- Legal issues must be carefully considered. Not all legal environments are the same. Care must be taken and advice considered—before commencing data collection or analysis—to ensure that planned procedures are allowed from a

legal perspective and that any evidence gathered may be used for legal purposes if required.
- Data collection across national borders must be done with proper legal advice about the export of data or about the type of data being collected.

Many of the forensic technology techniques described in this chapter were considered exotic just a few years ago, but today they have become routine practices in major investigations of all types, from pure cybercrime investigations that track hackers through compromised networks to the more common, but equally complex, forensic accounting investigations designed to identify fraud in the books and records of large corporations. Given society's dependence on computing technology, it is reasonable to anticipate that our reliance on data mining in investigations will only increase.

One can broadly consider the likely near-term evolution of data mining for investigations in two ways: technological advances in corporate IT systems and communications technology, and advances in data mining and fraud detection technologies.

Technological Advances in IT Systems and Communications Technology

Two of the most significant trends in corporate IT and communications likely to affect data mining are the advance of cloud computing and the increase in use of social networking technologies and collaborative tools in the corporate environment. First, both large and small corporations are evaluating cloud computing to reduce cost and increase flexibility in their IT environment. However, the mechanics of preserving and extracting data from a system housed in a cloud environment are not always well defined when corporate IT departments are considering moving to a cloud. Second, employees are increasingly communicating with each other and with business partners over systems other than e-mail—primarily social networking sites and collaborative tools like wikis. While the use of these techniques, as well as the tools to capture data from them, continue to evolve, one should consider whether to include them in the scope of an investigation.

Advances in Data Mining and Fraud Detection Technologies

Changing criminal tactics, the anonymity of e-commerce, and, as pointed out earlier, continuous introduction of new technologies and collaborative tools in the corporate environment all make fraud detection a constantly moving target. As such, data-mining tools will also continue to evolve, incorporating innovative data collection and analysis techniques.

For example, social network analysis may be deployed to gather social relationships in terms of ties presented on social networking sites, to be used as a component in further analysis. Text mining, a process of converting unstructured text into structured data objects, may be incorporated into the structured predictive models to improve performance. And the analysis models themselves are evolving to include more complex statistical techniques and predictive modeling (for example, neural networks).

Besides the more powerful and innovative analytics, advances in the field of fraud investigations include enhancements of the investigation life cycle itself. Automated case management systems offer rule-driven workflows for reporting, routing, and disposition of identified potentially fraudulent activities.

The only constant in forensic technology and data mining is change. By making use of the most up-to-date practices and procedures, forensic accounting investigators can work to stay one or two steps ahead of tech-savvy fraudsters.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 18

Report of Investigation

Thomas W. Golden and Ryan D. Murphy

Documenting an investigation is as important as performing it. A poorly documented case file can lead to a disappointing conclusion, can result in a dissatisfied client, and can even damage the financial accounting investigator's reputation and that of the investigator's firm. Various means by which the forensic accounting investigator may report his findings are discussed in greater detail in this chapter. The form of that report—whether oral or written—is a matter to be discussed with the client and with counsel. While it is not the responsibility of the forensic accounting investigator to advise on the legal perils associated with various forms of reporting, there are certain issues about which forensic accounting investigators should be aware as their clients debate the form of reporting that will conclude the investigator's investigation. This chapter addresses both written and oral reports of investigation.

We suggest that you discuss at the outset whether a written report is expected from you and, if so, its form and timing. In the common circumstance that this point cannot be decided at the inception of the engagement, you should conduct the investigation in a manner that will facilitate a comprehensive oral report, including the key documents and any exhibits necessary to illustrate the findings. Many investigations begin small, but there is no way to know with certainty where they will lead and what will be required at the conclusion. Although your client may not have requested a report at the outset of the investigation, some event in the course of the investigation may change the client's mind, and you should to be prepared to respond. For example, you may determine in the course of an investigation that an officer of the company violated a law or regulation, thereby requiring the company to consider self-reporting and possibly bringing a civil action against the officer and other third parties. Alternatively, you may be subpoenaed for your part in an investigation that has captured the attention of regulatory agencies or law enforcement. While you can testify only as to what procedures you recall performing and the attendant findings, your client—and your own reputation—will be better served if you have proper documentation. Our advice is to conduct an investigation as if you might be asked at a later time to report formally on your findings and on the procedures performed.

TYPES OF REPORTS

The following types of reports are relevant.

- Written reports
  - *Report of investigation.* This form of written report is given directly to the client, which may be the company's management, board, audit committee of the board, in-house counsel, or outside counsel. The report should stand on its own; that is, it should identify all of the relevant evidence that was used in concluding on the allegations under investigation. This is important because the client may rely on the report for various purposes such as corporate filings, lawsuits, employment actions, or alterations to procedures and controls.
  - *Expert report filed in a civil court proceeding.* We will touch on this topic only as it pertains to civil fraud court proceedings. The American Institute of Certified Public Accountants (AICPA) publishes an excellent practice aid on the full range of expert reports.[1]
  - *Affidavits.* These are voluntary declarations of facts and are communicated in written form and sworn to by the witness (declarant) before an officer authorized by the court.
  - *Informal reports.* These consist of memos to file, summary outlines used in delivery of an oral report, interview notes, spreadsheets listing transactions along with explanatory annotations, and other less-formal written material prepared by the investigation team.
- Oral reports
  - Oral reports are usually given by the forensic accounting investigation engagement leader to those overseeing an investigation, such as a company's board, or to those who represent the company's interests, such as outside counsel.
  - Oral reports may involve giving a deposition—as a fact witness or expert witness—during which everything that is said, by all parties to the deposition, is transcribed by a court reporter.

IMPORTANCE OF ADEQUATE PREPARATION

"I could have given you a more thorough and accurate report if I had had more time to prepare." The inexperienced forensic accounting investigator will no doubt say that at least once in a career in response to an irate client who is dissatisfied with a report on the preliminary results of an investigation. In our busy and complex world and in the course of a busy and complex investigation, not everything on the task list has the same priority. Experienced forensic accounting investigators know that any request for an update on an ongoing investigation is a report in the truest sense of the word *report.* One should not assume that an update delivered orally can be treated more casually than a written update. All reports deserve adequate preparation time and presentation in accordance with professional standards of practice.

[1] American Institute of Certified Public Accountants, Consulting Services Practice Aid 96–3, *Communicating in Litigation Services: Reports* (New York: American Institute of Certified Public Accountants, 1997).

Reporting is a critical responsibility of the forensic accounting investigator, and adequate preparation is necessary to present the status of the investigation in a manner that enables the decision makers to assess how to proceed. No report, oral or written, should be considered unofficial. Regardless of what you say or write to qualify your comments, once a document leaves your hands or words leave your lips, you cannot control the further distribution of the information you have communicated. Take the time to get it right.

STANDARDS OF REPORTING

Depending on your professional affiliations, you will be required to follow the reporting standards of your profession. If you are a certified fraud examiner (CFE), the applicable standards can be found in the *Fraud Examiners Manual*,[2] published for its members by the Association of Certified Fraud Examiners. If you are a certified public accountant (CPA), you should follow the reporting standards required for consulting engagements and found in the AICPA's *Statement on Standards for Consulting Services*.[3] If you are both a CFE and a CPA, you will be required to follow the standards of both associations. Because the AICPA standards are quite broad, while the standards of the Association of Certified Fraud Examiners (ACFE) are specific to fraud investigations, there is unlikely to be contradictory guidance if both professional standards are followed.

AICPA Consulting Standards

CPAs are required to follow the AICPA statement on standards for consulting services (SSCS), formerly known as statement on standards for management advisory services (SSMAS). The SSCS provides guidance for its members regarding certain types of consulting services. Section 100 of the AICPA professional standards contains the applicable guidance for CPAs who are performing consulting services, which encompasses essentially any professional service performed by members that is other than an examination, audit, review, or compilation.

The AICPA provides no specific reporting standards for consulting services per se and instructs members to look to the general standards of the profession, contained in Rule 201 of the AICPA code of professional conduct. Those standards are the following.

- *Professional competence*. Undertake only those professional services that the member or the member's firm can reasonably expect to complete with professional competence.
- *Due professional care*. Exercise due professional care in the performance of professional services.

---

[2] Association of Certified Fraud Examiners, *Fraud Examiners Manual* (Austin, TX: Association of Certified Fraud Examiners, 2002).

[3] American Institute of Certified Public Accountants, *Statement on Standards for Consulting Services* (New York: American Institute of Certified Public Accountants, 1991), codified in AICPA Professional Standards—Consulting Services: Definitions and Standards—CS § 100.

- *Planning and supervision.* Adequately plan and supervise the performance of professional services.
- *Sufficient relevant data.* Obtain sufficient relevant data to afford a reasonable basis for conclusions or recommendations in relation to any professional services performed.

In addition to the general standards applicable to all members, the AICPA stipulates additional general standards for all consulting services, promulgated to address the distinctive nature of consulting services in which the understanding with the client may establish valid limitations on the practitioner's performance of services. Those standards are established under Rule 202 of the AICPA code of professional conduct:

> Client interest. *Serve the client interest by seeking to accomplish the objectives established by the understanding with the client while maintaining integrity and objectivity.*[4] *Integrity requires a member to be, among other things, honest and candid within the constraints of client confidentiality. Service and the public trust should not be subordinated to personal gain and advantage. . . .*[5] *Objectivity is a state of mind, a quality that lends value to a member's services. It is a distinguishing feature of the profession. The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflicts of interest. Independence precludes relationships that may appear to impair a member's objectivity in rendering attestation services.*[6]
>
> Understanding with client. *Establish with the client a written or oral understanding about the responsibilities of the parties and the nature, scope, and limitations of services to be performed, and modify the understanding if circumstances require a significant change during the engagement.*[7]
>
> Communication with client. *Inform the client of* (a) *conflicts of interest that may occur pursuant to interpretations of Rule 102 of the Code of Professional Conduct,* (b) *significant reservations concerning the scope or benefits of the engagement, and* (c) *significant engagement findings or events.*[8] *A conflict of interest may occur if a member performs a professional service for a client or employer and the member or his or her firm has a significant relationship with another person, entity, product, or service that could be viewed as impairing the member's objectivity. If this significant relationship is disclosed to and consent is obtained from such client, employer, or other appropriate parties, the rule shall not operate to prohibit the performance of the professional service. . . .*[9]

---

[4] Statement on Standard for Consulting Services, CS § 100.07.
[5] Notes to CS § 100, Note 2, Article III of the Code of Professional Conduct, ET § 54, par. 2.
[6] Notes to CS § 100, Note 2, Article IV of the Code of Professional Conduct.
[7] CS § 100.07.
[8] Id.
[9] Notes to CS § 100, Note 3, Interpretation of 102–02.

AICPA SSCS says the following about performing consulting services for attest clients:

> *The performance of consulting services for an attest client does not, in and of itself, impair independence. However, members and their firms performing attest services for a client should comply with applicable independence standards, rules, and regulations issued by the AICPA, the state boards of accountancy, state CPA societies, and other regulatory agencies.*[10]

The concluding caveat, warning members to comply with "other regulatory agencies," serves to direct members to, among other things, the requirements of the Sarbanes-Oxley Act, which prohibits the performance of certain consulting services for attest clients (see Chapter 11).

ACFE Standards

The ACFE Reporting Standards are included in the *Fraud Examiners Manual*, a comprehensive guide designed specifically for use by members of the ACFE. (The *Fraud Examiners Manual* is also available to nonmembers.) Unlike the AICPA's rather general rules, ACFE reporting standards document a basis for reporting the results of a financial crimes investigation in a practical manner that can aid the forensic accounting investigator in preparing reports. The standards, both broad and detailed, give the forensic accounting investigator an overview of conceptual objectives as well as enough detail to guide both the novice and the experienced professional in reporting matters. The following points reflect ACFE reporting standards.

Preparation Do not expect to generate a well-written report from a poorly performed or poorly documented investigation. If the investigation has been performed and documented properly, then the reporting of procedures and findings should flow as a natural extension of the investigation. Preparation is critical to the reporting process and serves as the foundation for the other reporting standards. Preparation requires organizing each stage of the investigation from the initial engagement letter and data gathering to analysis and corroboration. Deficiencies in performing the investigation are likely to be very evident in the investigation report.

Accuracy It goes without saying that all reporting should be accurate. Accuracy applies not only to the information conveyed in the report, no matter how incidental, but also to the mechanics of communication: grammar, spelling, and the like. Mistakes in your report, however trivial, could cast doubt on the credibility of information that you know to be decisive. Accuracy in reporting basic data, dates, events, and names is critical.

Clarity Use clear and simple language to eliminate to the greatest degree possible any doubt about your intended communication. Written communications should be crafted in such a way that an average group of citizens selected for jury

[10] CS § 100.09.

duty could understand the facts and their interpretation. Because forensic accounting investigators are fact finders, the fact pattern described in the report should make the evidence clear, thus enabling the trier of fact—the individual (judge) or group (jury) rendering a decision—to reach the proper conclusion. You are there to assist them.

Impartiality Bias destroys credibility. The AICPA SSCS rules on integrity and objectivity, discussed earlier (see CS 100.07), parallel the impartiality requirement of the ACFE reporting standards. As a fact finder, the forensic accounting investigator contributes a crucially important set of findings to the trier of fact. Any perception of bias detected in reports may destroy the credibility of reported facts and thereby render the forensic accounting investigator's work less useful. Opinions as to culpability in criminal matters should not be stated. Subjective opinions and impressions often express unstated (or stated) bias and have no place in reporting, oral or written. The facts must speak for themselves.

Relevance Every investigation uncovers information that is irrelevant to the issues at hand. The report should include only facts relevant to resolving the allegations being investigated. Not only is irrelevant information distracting to recipients, but also the forensic accounting investigator's credibility may be at risk by implying flawed judgment as to what really matters.

Timeliness The report, as well as information gathered in support of it, should be submitted in a timely manner. This point is especially true of interviews that, if not documented and reported upon without delay, may cause decision makers to be less influenced by their contents.

The Written Report of Investigation

Needless to say, reports documenting an investigation differ considerably from audit opinions issued under Generally Accepted Auditing Standards (GAAS). The investigative report writer is not constrained by the required language of a governing standard, and investigative reports differ from one another in organization and content depending on the client's stated needs. In contrast, audit reports adhere to a set formula prescribed by GAAS. The uses of written reports also differ. The client could do any of the following things with an investigative report, among others.

- Distribute the report to a select group of individuals associated with the company in various capacities.
- Voluntarily give the report to a prosecutor as a referral for prosecution.
- Enter the report as evidence in a civil fraud proceeding.
- Give the report to outside counsel for use in preparing regulatory findings, entering negotiations, or providing other legal services on behalf of the company.

Whatever the ultimate fate of the written report, its basic elements will be much like the following elements.

Basic Elements to Consider for Inclusion in a Report of Investigation[11]

- Identify your client:

  [Firm] was engaged by Cutting Edge Technology Corporation (the Company).

- In the case of a lawsuit, identify the parties:

  I, [forensic accounting investigator's name], have been retained by [name of law firm] (counsel) to investigate certain of the claims and allegations made by Philip Hart (Hart), John Harrington (Harrington), and Robert Geller (Geller) against Peter Langley (Langley).

- State in broad terms what you were asked to do—for example, "to provide expert testimony or investigate certain allegations":

  . . . to provide forensic accounting investigation services in order to assist in pursuing your concerns related to certain allegations made against Jane Branford (Branford) and Phyllis Long (Long), general manager and chief financial officer, respectively, of the Company's Houston office.

- Describe your scope, including the time period examined:

  I was engaged to perform investigative procedures related to review of the Company's purchasing and receiving policies and practices in effect over fiscal years 2001 to 2003. We have performed background checks of certain employees at the direction of [name of outside counsel], reviewed and analyzed certain of the Company's accounting records and other documents, performed various data mining and data interrogation of the Company's electronic files, and conducted interviews of current and former Company employees.

- Include mention of any restriction as to distribution and use of the report:

  This report was prepared in connection with the aforementioned matter and is intended solely for your information. It may be used only for the purposes of this engagement and may not be used for any other purpose without our written consent.[12]

---

[11] This excludes certain reports following established reporting requirements such as Rule 26(b) of the Federal Rules of Civil Procedure.

[12] You might consider indicating that if you are presented with a subpoena, you will inform the client that you intend to comply unless the client makes court filings in an attempt to quash the subpoena.

- Identify the professional standards under which the work was conducted:

  We performed our work in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement on Standards for Consulting Services and the Association of Certified Fraud Examiners (ACFE) Fraud Examiners Manual.

- Identify exclusions in the reliance on your report:

  Our work does not constitute either an audit performed in accordance with the AICPA's Generally Accepted Auditing Standards or an attestation service. We make no representation as to the adequacy of our procedures for your purposes.

- State that your work should not be relied on to detect fraud:

  Fraud and irregularities by their very nature are most often hidden, and no absolute assurance can be given that all such matters will be detected. Our engagement cannot be relied on to disclose all irregularities or illegal acts, including fraud that may exist. During the course of this engagement, we will inform you of any such matters that come to our attention unless they are clearly inconsequential.

- Include the procedures you performed, technical pronouncements relied upon, and findings.[13]

  Work Performed and Observations *With respect to the issues expressed here, we performed the following work:*

  Considered the following accounting literature:

  Accounting Research Bulletin (ARB) No. 43, Chapter 4, Inventory Pricing

  Accounting Principles Board (APB) No. 20, Accounting Changes

  Statement on Auditing Standards No. 73, Appendix C, Statement of Position 85–3, Accounting by Agricultural Producers and Agricultural Cooperatives

  Reviewed the Company's financial statements and U.S. Securities and Exchange Commission filings

  Conclusions Based on Work Performed *Based upon our work and observations as described further on, the use by the Company—either as a grower of fruit for resale or as a juice manufacturing concern—of the specific identification method approximating first in, first out (FIFO) appears reasonable.*

[13] If appropriate, also perhaps include the implications of your observations and findings.

Properly performed the specific ID method matches the costs incurred to the actual physical flow of goods used in the manufacturing process. We found this to be the case in our review. We found no evidence supporting allegations that the company manipulated its inventory accounting records.

Generally Accepted Accounting Principles (GAAP) do not require growers, bottlers, or manufacturers to apply any specific inventory costing method. Neither does GAAP mandate a change in accounting method, as the Company altered its focus from that primarily of a grower to that primarily of a juice manufacturer.

The Company has contended that in the case where different pools of inventory were used, applying the specific ID method more accurately matched the true physical flow of goods, as these items are costed at the actual cost of the pool being consumed. Furthermore, the inventory on hand at period end is recorded at the cost of the items remaining in inventory. To the extent that inventory was used in the order in which it was grown or purchased, the use of specific ID in this regard approximated FIFO. Our procedures confirm the Company's position.

Flowcharts and exhibits within the body of the report or in the form of a referenced appendix will aid understanding. Refrain from including exhibits that are not referred to in the body of the report.

Summarizing Your Findings

A summary can be helpful to the reader but may be perilous for the report writer in regard to keeping critical information and perspectives intact. Caution is advised when preparing two types of summary sections: executive summary and conclusion.

We do not recommend writing a summary conclusion. If for any reason you nonetheless do so, be careful not to offer an opinion on the factual findings unless specifically requested to do so. The facts should speak for themselves. It may be appropriate to position in a concluding section of the Report of Investigation certain recommendations for additional investigative procedures or a description of control breakdowns you have observed.

Again, while we do not recommend summary conclusions, a carefully written executive summary at the beginning of the report can be extremely helpful to the reader, especially when it precedes a long and complex report. The executive summary should offer in simple, straightforward language an accurate statement of significant findings. Each summarized finding should include a reference to the full description of findings included in the complete Report of Investigation. Exhibit 18.1 provides an illustration.

WRITTEN REPORT OF EXPERT WITNESS OPINING FOR THE PLAINTIFF ON A CIVIL FRAUD CLAIM

A report written for submission at trial or like proceedings, such as arbitrations, is beyond the scope of this text. Forensic accounting investigators required to author such a report should take direction from client counsel in preparing a report that

EXHIBIT 18.1 Sample Report of Investigation—Executive Summary

Executive Summary

As a result of our work, we have noted the following preliminary findings as summarized below. It is important to note that the evidence we have identified in this Report of Investigation suggests but in no way incriminates any individual or entity. This Executive Summary is not meant to substitute for our following Report of Investigation. A summary of the evidence we have reviewed suggests that:

- Clark and Kent skimmed at a minimum $2,500,000 in cash from the Atlanta Division from February 1999 through their termination on July 5, 2001. (See *Section A-1.*)
- Clark directed at least $1,280,000 in aggregate from the Atlanta Division to his brother's company, Built-Right Construction, and his father's company, B&B Construction, from 1999 to 2001. Invoice review and interviews with personnel indicate that the services provided by these two companies may not have been performed. (See *Sections B-3 & B-4.*)
- Approximately $8,500,000 was paid from the Atlanta Division to 26 construction companies during 1999 to 2001 (see *Section B-2*); $415,000 was attributable to companies in which "cut and paste" invoices were discovered in Kent's desk. (See *Section A-4.*)
- Clark, Kent, and Clark's brother also benefited financially through transactions involving petty cash and theft of store merchandise. (See *Sections A-9 & D.*)

Our analysis has utilized Company-provided documentation and files beginning when the Company acquired a 100 percent interest in the Atlanta Division in 1999. Due to the schemes noted, the size of the dollars at risk, and General Manager Clark's tenure of 26 years, we recommend that the Company inform the seller and expand the scope of this investigation to include the years when only a 50 percent interest was held.

Additionally, we recommend that further investigative procedures be conducted to resolve the allegations we present in our findings discussed next.

meets all of the requirements of Rule 26(b) of the Federal Rules of Civil Procedure or other such rules as may be applicable to their appearance.

In most forensic accounting investigations there is no need to provide expert witness testimony. The forensic accounting investigator may, however, be asked to testify as a fact witness. As indicated earlier, the forensic accounting investigator is principally a fact finder and reports facts in a straightforward manner so that others—judge, jury, audit committee, board of creditors, or other interested party—can interpret those facts and make determinations as to their implications, including compliance with laws and regulations. There are, however, instances in which the forensic accounting investigator may be asked to prepare a formal expert report to a court in advance of a planned court appearance, at which time the investigator is expected to testify as to findings and to offer an opinion on a civil fraud claim. An example of a civil fraud claim opinion follows.

In the example, the expert witness is a forensic accounting investigator with both CPA and CFE credentials. He conducted an investigation at the request of counsel representing the buyer of a manufacturing business. In the course of the investigation, he learned that most sales under the previous owner had been effected through the payment of kickbacks and bribes. When the new owner took possession, he was unaware of the pattern of kickbacks and bribes, and he refused to pay when he was approached by customers or their agents. Not surprisingly, sales dropped off

significantly. Through his lawyer he filed a civil lawsuit, including among his claims that the defendant seller had known of the kickbacks and bribes, had failed to disclose them, and had thereby materially damaged the buyer. The forensic accounting investigator was asked to opine on the civil fraud charge. Following is that section of his report:[14]

IV. Opinion

Based upon my review, it was evident to me that there were numerous disbursement transactions between Buildit Manufacturing (Buildit) and a number of its vendors prior to buyer's involvement, which misrepresented the proper business purpose of the transactions. That is, invoices were presented to Buildit for goods and services that had not been furnished. However, given the level of kickbacks and bribery within Buildit, the testimony of individuals, and other evidence, I believe that the preponderance of the evidence indicates that a fraud was perpetrated upon the buyer of Buildit. I base my conclusion on the following definition of fraud.

Fraud in the inducement

Fraud occurs when a misrepresentation leads another to enter into a transaction with a false impression of the risks, duties, or obligations involved; an intentional misrepresentation of a material risk or duty reasonably relied on, thereby injuring the other party without vitiating the contract itself, especially about a fact relating to value.

Misrepresentation

I believe that the seller made numerous misrepresentations to the buyer, which include:

- *Failure to disclose that at least $2,469,910 was paid to shell companies, thereby providing cash for bribes to be paid to the owners of the companies (Shell Companies) listed on page 3 of this report. No goods and services were provided in exchange for cash paid to these entities.*
- *Failure to disclose that these payments were made to companies owned by individuals that were employed by significant customers of Buildit.*
- *Incorrectly classifying the payments to the Shell Companies as "direct labor" and "materials" expense.*
- *Providing the buyer with financial statements that included misclassifications of both revenue and expense.*

In my opinion, transactions were created in such a way as to conceal the true nature of the expense. There may have been other misrepresentations made by the seller to the buyer. However, these examples, I believe, satisfy the preceding definition.

[14] The following illustration represents only a portion of the entire expert report prepared in accordance with Rule 26(b) of the Federal Rules of Civil Procedure.

Reliance

The misclassification and recording of the payments to the Shell Companies concealed material risks that were not known by the buyer. In my opinion, had the buyer known about the existence of kickbacks and bribes, he would not have gone forward with the purchase. The fact that the buyer did go forward with the purchase demonstrates reliance.

Value/Damages

I have not been asked to calculate damages. It is my understanding, however, that counsel has retained another expert to perform this task.

AFFIDAVITS

An affidavit is a written statement submitted in a legal proceeding. Affidavits should receive the same level of care as that given to more extensive written reports. Typically not as long as reports of investigation, they attempt to summarize salient facts or they are submitted as sworn testimony previously submitted in the form of the forensic accounting investigator's report of investigation. The forensic accounting investigator should carefully edit the affidavit so it accurately conveys his own thoughts. The investigator should use words and phrases that are terms of art to the accounting profession, not the legal profession. A poorly drafted affidavit signed by a forensic accounting investigator can diminish that investigator's credibility. Like the report of investigation, the affidavit is the work product of the forensic accounting investigator.

INFORMAL REPORTS

There are certain informal types of reports, the most common of which are memos to file and presentations. Because any communication, written or oral, may be discoverable, professional care should be taken to ensure that all communications are accurate and comply with the relevant reporting standards.

A memo to file is a standard approach to the documentation of important events and understandings at points in time. The purpose of such memos is to document certain events and facts in the working papers of the forensic accounting investigator. At times, clients may ask for copies of such memos as substitutes for formal reports. While some clients may insist on receiving the memos prepared during the course of the investigation as opposed to a written report, they should be reminded that a memo is prepared at a point in time and is not a substitute for a written report. Presentations are an informal manner of reporting the results of an investigation. Presentations have the attributes of both written and oral reports—and can be dangerous if prepared carelessly. A written report allows for the possibility of thoroughly explaining a finding and its impact. The very nature of a presentation is brevity—in the expectation that the presenter will flesh out the information summarized in the slides. When using the presentation format in lieu of a detailed written report, the financial accounting investigator should consider whether a page with a boilerplate statement of responsibility could serve to remind the audience of certain limitations (see similar material at the beginning of the earlier discussion on the written Report

of Investigation). Also, consider including a statement at the bottom of each page reading, "The accompanying statement of responsibility is an integral part of this presentation."

While oral reports may require less effort and therefore generate less expense for the client, preparation for an oral report should be no less comprehensive than for a written report. Planning an oral report also requires both designation of a member of the team to deliver it and a decision regarding other team members who should be present. It may be wise to have staff members present or at least nearby who are most familiar with the details of certain interviews and events so the staff members can be called on in the event that the client wishes more detail.

An advantage of oral presentations is that there is ample opportunity for the forensic accounting investigator to clarify points, and those receiving the report can seek clarification by asking questions and can convey their particular concerns then and there. The interactive aspect of oral reports is probably their greatest benefit.

In the context of financial investigations, reports can take many different forms. Due to the dynamic nature of financial investigations, stakeholders involved in the oversight of investigations or relying on the results may want interim reports, which, while preliminary, represent an important responsibility of the forensic accounting investigator. Interim reports or updates are more useful if they include both a summary of the procedures performed, with related findings, and an overview of recommended procedures and expected outcomes. Also, an interim report should record what, if any, obstacles have hindered the forensic accounting investigators in the performance of their work. Investigations are something like a black box for those who must evaluate the results. The more factual information investigators report, the better it is for their audience, who are the decision makers.

An illustration may help here. Let us say that forensic accounting investigators have been investigating allegations that a drug company paid kickbacks to physicians for favoring the company's products. About two weeks into the investigation, the audit committee calls a hastily planned meeting with the forensic accounting investigators and asks for an update. The partner investigator indicates that his team of three professionals has been in the field for two weeks and has incurred $100,000 in fees and expenses. The partner reports that to date, the team has found no evidence of wrongdoing. The audit committee is pleased to hear this report. However, this bare-bones summary report, while correct, hardly gives either a correct impression or the comprehensive status of the investigation.

Preferably, the partner leading the forensic investigation advises the audit committee that a day of preparation to assimilate information from the team covering planned procedures performed to date, obstacles encountered, findings to date, and recommended further procedures will be beneficial. During this fact-gathering stage, the partner may reevaluate previously planned procedures and identify others he intends to suggest to the audit committee. Now he is adequately prepared. He presents orally to the audit committee and includes the same information as before regarding fees and expenses, but he is also in a position to add the following: "We learned yesterday that the electronic general ledger file is missing some journal entries made during a critical period. We have our information technology forensic team working to rectify the problem and get us complete electronic files. We have also learned from several doctors whom we called randomly that they do recall being solicited by a company representative in a manner they felt was inappropriate. While we have

yet to find conclusive evidence of the alleged improprieties, the preliminary evidence does suggest an expansion of the scope of our investigation to include telephone interviews of most of the doctors likely to have been called and follow up with face-to-face interviews of those reporting that they received such calls." The partner could continue the update by citing other issues and possibly including change-of-scope recommendations.

The example here focuses on oral reports because the oral report is a form of reporting that is often treated too informally—that is, not with the same diligence of preparation and review that a written report generally receives.

GIVING A DEPOSITION

The forensic accounting investigator may be called on to give a deposition, which is testimony in the presence of a court reporter and sometimes a videographer. Giving a deposition is an important activity and should not be taken lightly. Your professional reputation is at stake. Everything you have done in the course of an investigation is likely to come under close scrutiny. Your analysis, findings, and conclusions—even procedures you determined *not* to perform—all may be questioned. Expect that opposing counsel has met with another forensic accounting expert and received coaching on questions to ask you. Opposing counsel is likely to use techniques that attempt to impeach your credibility. That is opposing counsel's job, and experienced attorneys generally are very good at it. Do not underestimate their ability to dissect responses and catch the unwary forensic accounting investigator in a contradiction. Be sure to spend adequate time with counsel who will be defending your deposition, and consider all of counsel's recommendations. If you take issue with any of them, work it out before the deposition. Surprises at the deposition are unwise. While we recommend that you dedicate time to training materials such as the videotape *Preparing for a Deposition in a Business Case*,[15] the following are general guidelines to keep in mind when you've been engaged to give a deposition.

Be Prepared

A mistake on the part of inexperienced forensic accounting investigators is to prepare inadequately. They may believe that because they have performed the investigation, merely telling someone about it will be a simple matter. Caution is the preferable attitude: Take depositions seriously, and take the time to prepare well. Scrutinize each working paper just before the deposition, even if you have previously performed a detailed review. Question yourself on findings and procedures as a final step in preparing for a deposition.

[15] Jeffrey A. Jannuzzo, *Preparing for a Deposition in a Business Case* (Albany, NY: Matthew Bender, 1983).

It's *Your* Deposition

The most important thing to remember is that it's *your* deposition. You are in control from the standpoint that no else knows the material of your report better than you do. Also, you can have a substantial impact on the tone and the pace of the deposition. For example, counsel may try to rush you through questions, but you are entitled to take the time required to formulate the best response to each question.

It is important to take the necessary time to prepare for your deposition. Remember that your reputation and your firm's reputation are at risk if you are ill prepared. Tell counsel approximately how much time you need to prepare, and do not waiver from this point. It is your deposition, and you should treat it according to your own and your firm's high standards.

During the deposition, if you do not understand a certain question or if opposing counsel asks compound questions that are confusing, either ask for the question to be rephrased or simply say that you do not understand. Counsel may try to make you uncomfortable by commenting that you should be capable of understanding and answering a question. Such a comment may seem intimidating. Do not be intimidated; respond with professional courtesy and politeness—especially in more heated situations. If the opposing attorney fails to rephrase the question suitably, you can always say, "I apologize, and I want to be as complete in my response as I can, but I don't understand your question and cannot properly answer until I do."

Objectives of a Deposition in Civil Litigation

A deposition is a form of discovery. The other side is permitted to "discover" what you did, what you learned, your opinions, if any, and their basis. You are required to be responsive to all questions, but you need not volunteer any information that has not been requested. You will not convert the opposing lawyer to your perspective, no matter how hard you may wish to try. You are not there to educate opposing counsel even if it is evident from the line of questioning that opposing counsel is confused. No points are scored for being witty, and witty responses may backfire. Stay true to your objective, which is to listen to the questions very carefully and to answer only those questions as honestly and succinctly as possible. Listen closely to the question and answer only the question asked.

You Are Being Measured

The deposition is probably the first opportunity for the other side to meet you. While you are in their presence, you are being measured. They are picturing you in front of the judge or jury, evaluating what kind of witness you will make at trial. They will notice your appearance, your demeanor, and your level of overall confidence. Introduce yourself to the other side as well as to the court reporter. Present your business card to them. As with any business meeting there is often casual discussion of various topics at the beginning: the weather, travel plans, and the like. Joining these discussions should be approached cautiously because one of them may turn into a discussion of the case and your role in it—"This must be your biggest case"—which is not an appropriate subject to discuss off the record. This advice also holds for casual

encounters with opposing counsel in the elevator or hallway. Project confidence, and watch what you say at all times.

Without question, you are required to be honest and not withhold information; it is perfectly acceptable to say, however, "I don't know" if in fact you don't. Granted, we have heard tales of witnesses who, when they are trying to hide some incriminating facts, say they don't recall or they don't know. This is not what we mean to suggest here. It seems that one of the toughest things for some professional advisors to say is "I don't know" to a question put to them in an area they did not investigate or should not be realistically expected to comment on. They believe that an admission of ignorance will make them look weak, so they make the mistake of speculating, which in most cases is not a good idea. Unless you are specifically asked to speculate, you should not. Opposing counsel is free to ask questions and probe—sometimes in an effort to get you to speculate—or to ask for an opinion. You may hear the following, for example, from opposing counsel: "Well, wouldn't you expect the CFO [chief financial officer] to be informed about such matters?" This question calls for your *opinion,* not a report of your *factual findings*. As with all questions, you must respond truthfully. If you had such an expectation, you must say so. If, however, you have not formed opinions about what *should have happened*—as opposed to reporting your discoveries of what *did happen*—you should say so. Counsel may try to make you feel you *should* know by following up with a comment along these lines: "You told us just a moment ago that you have been a CPA for 20 years and have done hundreds of audits. Shouldn't you know the answer to this question?" Do not be intimidated; you have no obligation to know what others were hoping you would know or were hoping would be within the scope of your work. Often, the worst thing you can do is to assume or speculate in response to a question when you really do not know the answer. You are not expected to have a photographic memory. In this regard, you may wish to consult with counsel about preparing a binder containing the most relevant materials from the investigation, precisely because you are unlikely to remember every detail of a complex case.

Reviewing Your Deposition Transcript

Generally, each person deposed may review the deposition transcript for any errors made by the court reporter and then sign the deposition after noting any corrections necessary. Counsel establishes different protocols in different cases, and accordingly, you may be asked to waive signature at the conclusion of your deposition. This means that the deposition will stand as transcribed—without your review. Counsel can advise you in advance of the practice in the particular case, and if you are unsure whether or not it is acceptable to you, discuss it with counsel. Whether signature is waived or not, it is important to read your deposition transcript with several objectives in mind. First, you want to ensure that what you said was transcribed correctly. Second, you may notice an inaccurate response unknown to you at the time but now evident as you review your comments. Third, opposing counsel's questions and your testimony may identify a weakness in your investigation for which you will want to be prepared at trial. And if you gave a response that was factually inaccurate, you will want to advise counsel of the error. Even if you believe the deposition went well, take time to read it thoroughly.

Other Considerations

One of the best ways to ensure a successful deposition is to spend adequate time with the attorney who will be defending your deposition. No two depositions are alike, so even if you have given a number of them, you must still become acquainted with your counsel's strategy for the deposition. Also make sure counsel defending your deposition knows the limitations of your knowledge and expertise. Again, the deposition is not the place for surprises. Based on the experience of the authors, the following are additional considerations.

- Think before you speak. The deposition transcript bears no indication of the time it takes you to respond to a question. Once said, words cannot be deleted from the deposition transcript.
- Be cautious in responding to questions that contain absolutes such as *never* or *always*.
- Avoid clever sound bites that may be used against you at trial.
- Speak in complete sentences, using proper grammar in a lucid manner at an ordinary speed. That will enable the court reporter to record your words accurately.
- Pause before each answer, no matter how confident you are of your answer. That allows you to repeat the question silently to yourself and gives counsel defending your deposition time to enter an objection if counsel cares to do so.
- When asked to comment on an exhibit, if time to read it isn't offered, ask permission to read it before responding. Make sure you are familiar with it, and if you are not, state that for the record. You have the right to read every document presented before responding to questions about it. Opposing counsel may seem annoyed at your request to read a document, but despite that discontent it is generally advisable to make sure you know what a document says before answering questions about it.
- Be specific in your answers, and do not exaggerate. For example, if you are asked, "Have you ever audited a financial institution before?" and your answer is, "Sure, a great many," do not be surprised if opposing counsel pulls out a sheet of blank paper, gets ready to start writing a list, and says, "Please tell me the name of the first financial institution you audited, your responsibilities in that engagement, and when that occurred." If it is true that you have audited "a great many," opposing counsel would expect to write down a very long list. If your experience includes eight financial institutions, you may think eight is a great many, but others may think of eight as only a few. The better reply to the initial question may be, "Yes, I have."

If you are properly prepared, giving a deposition is somewhat similar to an oral report, although not often organized in the manner you would select. Remembering that your comments will become a written transcript and that your spoken words, once transcribed, can never be taken back, should instill in you the importance of adequate preparation.

MISTAKES TO AVOID IN REPORTING

The following brief discussions highlight and review issues raised earlier in this chapter.

Avoid Overstatement

In the memorable TV series *Dragnet,* Sgt. Joe Friday used to say, "Just the facts, ma'am." The same holds true when it comes to reports of investigation. The closer one sticks to the facts, all the facts, and just the facts, without embellishment, the better the report. The facts should speak for themselves. This is not to say that all facts are created equal: Some facts are smoking-gun discoveries—for example, memos demonstrating both knowledge and intent. However, even in respect of obviously important facts, be careful not to overstate them.

Avoid Opinion

Other than the engagement to serve as an expert witness in a civil matter, the forensic accounting investigator should not offer opinions about the matter at hand. Also, opinions as to the intent or culpability (in criminal matters) of certain persons or as to whether an act was in fact a fraud should be avoided. These are matters to be decided by the trier of fact based on the factual material gathered and presented by the forensic accounting investigator. The forensic accounting investigator should not endeavor to influence the outcome beyond presenting the findings of the investigation in a clear and logical order.

Identify Control Issues Separately from Investigative Findings of Fact

Your client may often ask you to identify control issues spotted during the course of your investigation. While appropriate to include in your report, we suggest including them in a separate section so as to focus on your primary task, which is that of a fact finder. The discovery of facts, leading to the resolution of potential criminal issues, is the forensic accounting investigator's professional calling. Identifying control breakdowns is a natural by-product of a fraud investigation, but such breakdowns should be addressed in a separate section of the report.

What does it mean in practice to give precedence to the pertinent facts? An example: A number of laptops are missing, and several of them can be traced directly to your target. If you actually wanted to give precedence to the control issue, you would write, "The control over laptop assignments is weak, and it was therefore impossible to account for all laptops acquired by the accounting department." But if you put your focus where it belongs, you would write something of the following kind: "Over the past year, 11 laptops were purchased by accounting and assigned to ten individuals, including two to the controller. When questioned, the controller showed us one of the laptops and could not account for the other."

Use Simple, Straightforward Language Focused on the Facts

The task of the forensic accounting investigator is to take a complex situation, properly investigate it to determine the relevant facts, and then report those facts in a simple, straightforward manner so that the reader or person hearing the report understands the facts and how they should be interpreted for resolution of the allegations. Who was involved? How much damage was caused? How did the events occur? Why did the company not catch the problem earlier? In reporting the answers to these questions, there is no room for speculation.

Again, let us reduce these observations to an example. We would not recommend writing as follows: "The CFO admitted to recording false revenue but said he didn't mean to hurt anyone. He wanted to keep the numbers up so that the division would not be closed." Text similar to the following may be preferable: "The CFO admitted to generating false revenue in an effort to achieve budgeted sales figures. He admitted to making the monthly entries with full knowledge of the fact that he was deceiving corporate officials and that his actions were improper under GAAP and company policy. His stated reason for his action was his fear that corporate headquarters would close the division and lay off a large number of employees in his division."

Avoid Subjective Comments

As a fact finder, the forensic accounting investigator must restrict comments to presentation of the facts in such a way as to resolve the allegations that occasioned the original engagement.[16] The investigator may give opinions about standard and customary business practices that relate to the observed behavior but not directly attempt to characterize the facts as discovered. The investigator should simply report them. If the finding is, for example, that the executive director of a charity has taken a number of trips, reportedly for business purposes, accompanied by family members, the investigator should not characterize such trips as excessive or without business purpose but should report only the facts. Those reading or hearing the facts can evaluate them in light of organizational policies and applicable laws and regulations.

In the written or oral report, how should the forensic accounting investigator convey an understanding of the facts? We would not recommend the following: "We noted that the executive director took *excessive* trips to New York with his family, which were *inappropriate* and *unrelated to the business of the organization,* although he expensed the trips as business related." The foregoing is replete with errors.

- *Excessive.* The word *excessive* is judgmental and appears to reflect the personal standard of the forensic accounting investigator. Synonymous words—such as *abusive, unacceptable,* and *extravagant*—are also judgmental characterizations and may not have a valid place in your report.
- *Inappropriate.* This term characterizes the observed action and should be avoided. It conveys a conclusion, not a fact. In the strictly factual realm, the

[16] As discussed earlier in this chapter, opinions by the forensic accountant are permitted if engaged as an expert in a civil fraud matter.

report could note that such travel took place, that it required approval by the individual's supervisor, and whether or not the required approval was sought or given. The report could also reference a specific provision of the organizational policy handbook to document the requirement. Each of these facts would enable readers of the report to characterize the subject's actions—and those readers are then more than likely to deem the actions inappropriate. But that is *their* role, not the forensic accounting investigator's role.

- *Unrelated to the business of the organization.* Such statements are usually made on the basis of assumptions. More likely than not, the trips were indeed unrelated to the organization's business, but it would be wrong to characterize them as such. The investigator should report either that no business purpose was discovered or that the individual admitted in an interview that he knew the trips were strictly personal. Either of these statements may be a better manner of reporting. They report facts, not characterizations.

WORKING PAPERS

Given the familiarity that most auditors have with working-paper-documentation techniques, many of which are applicable to forensic investigation, those techniques are not discussed at length here. However, certain techniques are especially pertinent to investigation, as the following pages demonstrate.

A forensic accounting investigator, once engaged, needs to take certain internal steps to document procedures, findings, and in some cases, recommendations. These elements of the investigation process are documented in a collection of evidence termed *working papers,* which divide into two broad categories: internal, or administrative, and substantive work product.[17]

Forensic accounting investigators naturally want legitimate protections over their work, such as liability limitations and work product privilege, when applicable. Here are a few important tips for achieving those goals. Judgment, as always, is needed here—these tips are not applicable in all cases—but generally speaking, we advise the following measures.

Signed Engagement Letter

It is always best to begin the engagement only after you have a signed engagement letter in hand. While there are exceptions to this rule, they should be rare. Even if the client states you will receive it on the first day of fieldwork, insist on having it faxed to you before traveling to the client site. The client is often not focused on engagement administration when there is a need to get the investigation going, but from your standpoint that is exactly the time to get the paperwork done. A client

[17] Merriam-Webster's *Dictionary of Law 1996* defines *work product* as "the set of materials (as notes), mental impressions, conclusions, opinions, or legal theories developed by or for an attorney in anticipation of litigation or for trial." Definitions vary from jurisdiction to jurisdiction.

that knows you will not begin the investigation until the engagement letter is signed will be motivated to complete this aspect of engagement administration to set the investigation in motion.

The engagement letter should address a variety of items. They include but are not limited to the scope of services, timing of the work, the deliverable (written or verbal report), fee structure, governing law and jurisdiction, and limitation of liability. In some situations, the engagement letter will be addressed to the law firm as the client.

Engagement letters for investigations differ in several respects from audit engagement letters, most notably in the treatment of liability protections for the forensic accounting firm, for example, as follows:

> Liability limitation and indemnification. *In no event shall [name of forensic accounting firm] be liable to you or your client—whether a claim be in tort, contract, or otherwise—either for any amount in excess of the total professional fees paid pursuant to the engagement letter or any addendum to which the claim relates—or for any consequential, indirect, lost profit, or similar damages related to [name of forensic accounting firm]'s services provided under this letter of engagement except to the extent finally determined to have resulted from the willful misconduct or fraudulent behavior of [name of forensic accounting firm] related to such services.*
>
> *You and your client agree to indemnify and hold harmless [name of forensic accounting firm] and its personnel from any and all third-party claims, liabilities, costs, and expenses related to services [name of forensic accounting firm] renders under this engagement letter except to the extent finally determined to have resulted from the willful misconduct or fraudulent behavior of [name of forensic accounting firm] related to such services.*

While this contract provision is not allowed by the U.S. Securities and Exchange Commission for purposes of performing an audit, it is an important provision in a financial investigation. For audit services, the auditing firm determines the scope of the engagement in keeping with regulatory and professional standards, industry norms, and its own professional judgment. The company turns over its financial statements and supporting documentation, books, and records and allows interviews of its employees, observations of assets, and inquiries of third parties by the auditor. In the event of an undue attempt by management to restrict the scope of the audit, the auditor may modify the audit report (scope limitation) or resign the engagement.

Matters differ for forensic accounting investigators. While investigators certainly make recommendations as to scope and procedures, they are essentially working at the direction of others. The client is responsible for conducting the investigation, and the forensic accounting investigator is, so to speak, a tool at the client's disposal. The provision discussed earlier is intended to protect the forensic accounting investigator from claims that an investigation was not properly performed or that individuals were harmed as a result of the investigation.

Given the sensitivity of the issues covered in the engagement letter, you may now agree more fully than at the beginning of this discussion that it is best to have a signed engagement letter before setting to work.

RELATIONSHIP REVIEW

Most firms that provide forensic accounting services have their own procedures for performing a relationship review, or conflicts check—that is, identifying relationships that the firm may have had or now has with any of the parties involved. The points reviewed and documented may well include the following:

- The date on which the relationship review was cleared
- The individual who cleared it
- Notations of pertinent discussions in clearing current and prior relationships
- The date on which the assignment was accepted

For forensic accounting investigators to become familiar with a specific company or situation, they may perform some background research such as checking the Internet, performing a public records search, obtaining a Dun and Bradstreet report, and searching various fee-based databases. However, no investigative work of substance should begin before the relationship check has cleared. Identifying a conflicting relationship that may preclude a firm from accepting the assignment after work has begun reflects negatively on the practitioner, the firm, and even the client, especially if court-imposed deadlines—such as deadlines for naming experts—have passed.

SUBSTANTIVE WORKING PAPERS

Depending on the assignment, substantive working papers in either hard copy or electronic form may include many different items. If the work is being performed under privilege (see Chapter 20), all working papers should be clearly marked to that effect.

The practitioner should endeavor to prepare working papers as though a third party or regulatory authority may seek to review them. It is not the task of the forensic accounting investigator to assert the privilege or contest subpoenas; the forensic accounting investigator's task is to maintain its viability of privilege should counsel decide to assert it and likewise to advise counsel if subpoenas are received so counsel can decide whether to contest them. Exhibit 18.2 is an example of a working paper clearly marked with the designation "Privileged, Attorney Work Product" to help identify it as a privileged communication.

EACH WORKING PAPER SHOULD STAND ON ITS OWN

Any working papers created by the engagement team should be clearly marked to indicate the name of the creator, the date, the source of information, the information's classification, and the issue addressed. Such working papers should also be secured so as to ensure that only members of the immediate engagement team have access to them. Certain matters will require the forensic accounting investigators to prove that they have used reasonable means to secure from others the working papers and

EXHIBIT 18.2 Privileged Work Product

Check Number	Amount	Check Date	Vendor Number	Full Name
394795	$56,117.80	5/4/2000	3D SYSTEMS	Johnson Safeguarding
400341	$56,117.80	6/29/2000	3D SYSTEMS	Johnson Safeguarding
401256	$56,117.80	7/27/2000		Johnson Safeguarding
402004	$56,117.80	8/30/2000		Johnson Safeguarding
393821	$15,545.00	1/3/2000		Reed Diagnostics
394002	$15,545.00	2/6/2000		Reed Diagnostics
394211	$15,545.00	3/8/2000		Reed Diagnostics
394526	$15,545.00	4/4/2000		Reed Diagnostics
394701	$15,545.00	5/2/2000		Reed Diagnostics

Attorney Work Product
DRAFT—Tentative and Preliminary
Privileged and Confidential

other evidence. In such matters, custody can be proved by ensuring that working papers be kept in a secure room with a sign-in sheet for all who have access to the room.

If a working paper was prepared by the client, it should be so designated, usually by the initials PBC (for *prepared by client*). If the purpose of a working paper is not evident upon inspection, a simple note of explanation should suffice. The purpose of a complete set of working papers, as noted earlier in the chapter, is to document the forensic accounting investigator's work, which should be planned and performed in the expectation that a report will be issued at the conclusion of the engagement even if not specifically requested at the outset. The importance of marking the origin of material in the working papers was illustrated in a case that spawned 11 years of litigation—*Mattco Forge v. Ernst & Young*. In this matter, the accounting expert's request that missing job cost estimate documents be recreated was done without noting that the documents were not created in the normal course of business. The client Mattco believed this had impaired their success at trial on the merits of the case and sued Ernst & Young for damages of approximately $40 million. While this matter was ultimately resolved in favor of the accountant and the accounting profession, it is a cautionary tale about the need to clearly record the nature and source of documentation on which the forensic accountant relies in the course of an investigation.[18]

Numerical amounts or other relevant data should be cross-referenced using the to/from format. The cross-reference on the left should indicate where the number is coming from—for example, an invoice—and the right cross-reference should indicate where it is going to—for example, another schedule or the Report of Investigation. Working papers using this format will tend to have an even flow, such that an independent reviewer will have little difficulty in understanding the nature of support for the conclusions ultimately reached.

[18] Wayne Baliga, "Victory for CPAs in Litigation Services," *Journal of Accountancy* 184, July 1, 1997.

Many of the preceding observations have made clear that working papers should be prepared in such a way that they are understandable to an independent reviewer. It is important from an efficiency perspective to consider that the purpose of the working paper is to document procedures performed and conclusions reached. Neatness, while desirable, is not an end in itself; if it is understandable, then it is acceptable. The most efficient method to make corrections should be used. In many instances, that method will entail simply writing on it. Redoing the entire working paper may be unnecessary. Working papers need not be typed or formal. They are intended to document your work. That is all. If the document you create is clear, accurate, and readable, it qualifies as a working paper.

TESTIMONY BINDER

A forensic accounting investigator may be called upon to testify at a deposition. Depending on the complexity of the matter, you might consider preparing what is called a testimony binder to assist in your preparation for the deposition. This is a matter to be discussed with counsel before the deposition. Many find it helpful to refer to certain key documents when discussing their procedures and findings in the deposition.

INTERVIEW MEMORANDUMS

Documenting an interview is critical. If later evidence proves that the interviewer was inaccurate even on a seemingly insignificant aspect of the interview, the credibility of the interview memorandum may be called into doubt. Most experts advise against recording the interview in a question-and-answer format, because the format itself

EXHIBIT 18.3 Interview Memorandum: Opening Section

Duration: Approximately two hours
Interviewers: Bill Peters and Sulaksh Godrej
Location: Conference Rm 8-F, Lab Building, Chicago
Date: October 2, 2005
David has been with [the company] for 16 years and has primarily been responsible for the Chicago operations. He started with [the company] as vice president and treasurer and was primarily responsible for the company's consolidated financial statements. He has a staff of six accountants reporting to him. He was the president of the Chicago division from 1992 to 2002, and then the CEO from 2002 to 2003. At present, he is the CFO and treasurer of [the parent].
Before joining [the company] he was with [accounting firm] from 1978 through 1985 and left one year after promotion to manager. He focused mainly on the textile industry and served on the audit team for [the company] until he was offered to join [the company] in 1989 as controller of the Chicago division. He is an accounting graduate of Notre Dame, having passed the CPA exam on his first sitting in 1979. He is married and has two young children. His wife is not employed outside the home.

EXHIBIT 18.4 Interview Memorandum: A Defensive Interviewee

David was very defensive and adversarial throughout the interview. When he almost walked out of the interview at the very beginning of the questioning, Tom asked him:

> Q: Are you telling us that you are refusing to cooperate with this investigation, with the management of [the company]?
> A: All I am saying is I am not going to sit here and answer all your questions. I am a director and shareholder of this company and I will deal with the management directly. I want copies of your report and other supporting documents and I will address your concerns with the management.

He almost walked out of the interview more than once.

Throughout the entire interview, every time he was asked a question about a sticky point, before giving the answer he asked if we had an e-mail on the topic. The entire interview was a game of "Ask me the right question and I'll answer it"—which he did not. Toward the end of the interview, I told him that he treated this as a deposition when all I wanted was his help. He repeatedly said he would help, but he never told me anything I did not already know. Nothing. He insisted that he did, but when asked for one example, he could not come up with anything and eventually responded by saying, "Just read his notes," and pointed to my co-interviewer.

suggests a greater degree of accuracy than is usually necessary. You do not want to give the impression that it is a transcript. However, it may be useful for certain key responses as a means of providing appropriate emphasis and clarity. Exhibit 18.3 samples the opening section of an interview memorandum.

Interviewers' impressions of the witness's behavioral characteristics are appropriate. Exhibit 18.4 offers an example of this type of reporting and shows as well how the question-and-answer format can be used effectively for emphasis.

The sequence of the interview is best structured either by time or by topic. Exhibit 18.5 is an example of the witness's responses grouped by area of interest.

EXHIBIT 18.5 Interview Memorandum: Recording by Topic

- He understood the FCPA and was not aware of any payments made to government officials anywhere.
- Bribes to General in Thailand—Asked him several times about FCPA violations, specifically bribes. He denied any knowledge. After referring to the Southeast Asian business, I asked him again, and he said no. Then I showed him the e-mail. Asked if he remembered it. He reluctantly said, "Vaguely."
- Cuba—Before showing him the series of e-mails, he was emphatic that he knew nothing about any sales to Cuba. When I showed him the series of three e-mails, he still maintained that he had heard nothing about such a venture but then began to speculate about what probably happened: "Well, what I think is happening here is that Jon came up with an idea, which he often does, and then they all kicked it around." I said I did not wish to speculate about what might have happened, only tell me what he recalls. He recalled nothing about Cuba. Interestingly, he was prepared to walk out of the room until I said I had some questions about sales to Cuba. He then said, "All right, let me get some paper," whereupon he did so and returned. He took notes during the remainder of the interview.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 19

Supporting a Criminal Prosecution

Albert A. Vondra, Thomas W. Golden, John Gallo, and Isabel M. Cumming

This chapter addresses the issues your client and your client's counsel confront in evaluating when and how to refer a matter to a prosecutor for investigation of those believed to be involved in criminal acts.[1] U.S. Department of Justice (DOJ) guidelines lay out in unambiguous language the DOJ's desire for vigorous enforcement of criminal laws against corporate wrongdoers, including the corporation itself. The government's view is that indictment of corporations for wrongdoing in appropriate circumstances enables the government to be a positive force in changing the corporate culture in favor of a new paradigm of deterring, detecting, and punishing white collar crime. The environment has changed such that corporate cooperation with government prosecutions of illegal activity is becoming commonplace. The question of whether or not to report the crimes of individual employees when the corporation is the victim is an extremely important decision, and this chapter explores considerations related to it.

Our experience shows that many corporations find the decision to refer an errant employee for prosecution a difficult one because of the reality that prosecution can have long-lasting, widespread effects on the company. The decision as to whether or not to refer a matter generally rests with senior management and counsel, including the company's general counsel and, in some cases, the board of directors. In light of the many considerations discussed in this chapter and inherent in the decision to make a criminal referral, a very careful and sophisticated assessment should be made by senior management and counsel, aided and informed by the forensic accounting investigator as well as other experts as needed. Once a decision has been thoughtfully made, the company should act with conviction and see the decision through to the end.

[1] Throughout this chapter, we refer to prosecution as the right of a company or individual to inform a government law enforcement agency of a violation of the law. However, only the government can determine whether or not to prosecute a case. Our reference to prosecution by a company implies a referral to a governmental representative legally empowered with this responsibility.

KEY CONSIDERATIONS

The decision confronting management and counsel as to whether or not to move forward with a referral for prosecution often depends on many circumstances.

Deterrent Effect of Appropriate Response

Many companies have the view that violators should be prosecuted—in the belief that culpable parties need to be held accountable for their actions and punished "to the full extent of the law," and doing so will deter comparable acts by others in the future. This view continues along these lines: If an employee who perpetrates a significant fraud is simply demoted or terminated without being held criminally liable in court, the wrong message may be sent to the rest of the organization. In our experience, rigorously pursuing that well-chosen remedy is the true deterrent. The best practice is to communicate throughout the organization that if employees do something inappropriate, they will be caught and their punishment will be swift and commensurate with the crime. If a criminal referral is the appropriate remedy, the company should not hesitate to elect that option—and doing so will send a powerful message throughout the entire organization.

It is our experience that few things are more damaging to employee morale than to see that a company does not walk the talk. In recent years, many companies have gone to great lengths to promote ethical governance and conduct by all directors, officers, and employees of the company. For the most part, they have done an excellent job of formulating and communicating the importance of ethical behavior. However, employees are aware of whether and how the company walks the talk when actually responding to violations.

U.S. Sentencing Commission Guidelines

As noted earlier, in our experience the rigorous pursuit of a well-chosen remedy is the most successful deterrent to future instances of fraud. The U.S. Sentencing Commission in 1991 established organizational federal sentencing guidelines (FSG) that apply to corporations, partnerships, labor unions, pension funds, trusts, nonprofit entities, and government units (virtually all types of organizations). The guidelines set out criteria for corporate compliance programs, which are consistent with the rigorous pursuit of fraud. They require consistent punishment of individual wrongdoers, and can hold an entire organization criminally liable for illegal acts committed by the organization's employees.

Although no corporate compliance program can prevent all types and occurrences of fraud and wrongdoing, such programs must be well designed and vigorously implemented to maximize their effectiveness in deterring and detecting wrongdoing by employees. They cannot be just paper programs. The seven key criteria for establishing an effective compliance program, as outlined by the guidelines, are as follows:

1. Compliance standards and procedures reasonably capable of reducing the prospect of criminal activity
2. Oversight by high-level personnel

3. Due care in delegating substantial discretionary authority
4. Effective communication to employees at all levels
5. Reasonable steps to achieve compliance
6. Consistent enforcement of standards, including disciplinary mechanisms
7. Reasonable steps to respond to and prevent further similar offenses upon detection of a violation[2]

The guidelines were amended in 2004 to include ten modifications known as FSG II. Each item is intended to eliminate ambiguities from the original seven components of an "effective program to prevent and detect violations of law." FSG II was intended to synchronize the guidelines with both Sarbanes-Oxley and "emerging public and private regulatory requirements." The ten recommended modifications are:

1. *Tone at the Top*—Emphasize within the guidelines the importance of an organizational culture that encourages a commitment to compliance with the law.
2. *Conduct and Internal Control*—Provide a better description of *compliance standards and procedures*—namely, "standards of conduct and internal control systems that are reasonably capable of reducing the likelihood of violations of law."
3. *Leadership Accountability*—Specify the responsibilities of an organization's governing authority and organizational leadership for compliance.
4. *Resources and Authority*—Emphasize the importance of adequate resources and authority for individuals with responsibility for implementation of the program.
5. *History of Violations*—Replace the current terminology—"propensity to engage in violations of law"—with the more objective requirement of determining whether there has been a "history of engaging in violations of law."
6. *Conduct Training*—Include training and the dissemination of training materials and information within the definition of *effective program*.
7. *Evaluate Programs*—Add "periodic evaluation of the effectiveness of a program" to the requirement for monitoring and auditing systems.
8. *Whistle-Blower System*—Require a mechanism for anonymous reporting.
9. *Encourage Employees*—Establish a system whereby employees can both report actual violations and seek guidance about potential violations in order to more specifically encourage prevention and deterrence of violations.
10. *Risk Assessment*—Provide for the conduct of ongoing risk assessments as part of the implementation of an "effective program."[3]

---

[2] Throughout this chapter, we refer to prosecution as the right of a company or individual to inform a government law enforcement agency of a violation of the law. However, only the government can determine whether or not to prosecute a case. Our reference to prosecution by a company implies a referral to a governmental representative legally empowered with this responsibility.

[3] Throughout this chapter, we refer to prosecution as the right of a company or individual to inform a government law enforcement agency of a violation of the law. However, only the government can determine whether or not to prosecute a case. Our reference to prosecution by a company implies a referral to a governmental representative legally empowered with this responsibility.

Also in 2004, the Department of Justice released Opinion Procedure 04-02, which describes a number of precautions companies can take "to avoid, in the future, a knowing violation of the FCPA." This is described in more detail in Chapter 26.

Expense and Possible Outcomes

It is important to understand the time and financial commitment required, once management and counsel decide to refer a matter for prosecution. The most appealing case for any prosecutor is one that involves clear and simple facts. Because of limited resources, prosecutors at every level of government typically have no staff forensic accounting investigators and may not have the resources to pursue all of the cases presented to them. They must choose their cases wisely and select those most likely to yield a successful prosecution that furthers their primary responsibility of protecting the public interest. Because white collar crimes are often complex, they are sometimes perceived as having less jury appeal. Experience also shows that jurors often sympathize with white collar criminals, believing that through loss of a job and reputational damage, the defendant has been punished enough. However, recent business catastrophes bringing to the spotlight certain deceitful financial reporting practices have likely made the public much less sympathetic toward white collar criminals.

Forensic accounting investigators can assist the prosecutor in white collar cases. The forensic accounting investigator should be able to explain complex scams in simple, straightforward terms so that the great majority of jurors—even those without significant experience in corporate life—can understand the facts and how they should be interpreted. Even with the assistance of a forensic accounting investigator, there is, of course, no guarantee of a successful prosecution.

Referrals for Prosecution May Attract Public Attention

If the decision to refer a matter for prosecution is taken, it is our experience that the organization should be prepared for public inquiry as a possible consequence. Consider the following experience.

The director of a national charitable foundation stole $10 million from the organization before being apprehended and prosecuted. The entire matter unfolded before the public eye. Ultimately, nearly 80 percent of the stolen funds were recovered, but many news commentators and the public criticized the charity for hiring a bad apple in the first place, claiming the charity should have known better. The public was indignant: "How dare they play with the money of tens of thousands of contributors? I'll never again give to that organization." It happens that the organization had very strong controls—better than in many other companies. However, as most accountants know, when a senior executive perpetrates fraud, it is difficult to prevent it, let alone recover the funds.

The charity passed through its nightmare and eventually emerged quite strong again. Asked whether, in the end, he thought it had been wise to refer the matter for prosecution and bear the public's response, one of the organization's veteran executives—a principled elder statesman—had this to say: "If he had not been prosecuted, there was a strong likelihood that this relatively young executive would have found a job at another charity and stolen again. But we paid a high price by

disclosing to the public that we had been duped by one of our own. We risked the very survival of our mission, which is saving lives!"

This veteran executive teaches that the burden placed on society by a decision not to pursue prosecution may be significant. Because the overwhelming majority of employees who defraud their employers are terminated without prosecution, many remain in the workforce. Not surprisingly, some return to their devious ways. Had they been convicted of a crime at the first detected occurrence, future employers would more likely learn that this person should not be placed in a position of trust. Avoiding prosecution sends a criminal out into society to potentially prey on another victim.

REFERRAL CONSIDERATIONS

When referring a matter for prosecution is the course of action selected, a series of considerations remains regarding when to do so. In our experience these are issues for management and counsel to evaluate. Each case will present different issues, but a number of issues will likely arise and are considerations in deciding the timing of contacting the authorities. Among them are:

- Whether or not the investigation is sufficiently advanced to make a reasonably informed decision about the nature of the suspected crime
- What the specific laws or regulations related to the suspected crime, or the industry in which the entity operates, require of the company
- The level of the individual nature of the offense
- Whether or not the company's insurance coverage contains any clauses that would affect the timing of the referral

As noted earlier, there are many considerations confronting counsel about the timing of a referral. More often today, companies are deciding to self-report incidents at the early stages of their investigations followed by periodic updates to government enforcement officials such as the U.S. Securities and Exchange Commission. In our experience, reasons that may suggest a prompt referral include some or all of the following.

- There is a possibility that the company has violated laws or regulations, and it is advantageous under the relevant law or regulatory rules to self-report. In that case, time may be of the essence.
- The prosecutor may separately have commenced an investigation and could bring the forensic accounting investigator into his investigation under a 6(e) procedure that gives access to some or all of the prosecutor's evidence. This is explained more fully in Chapter 20 and may greatly facilitate both the public prosecution and the internal investigation and remediation efforts within the company.
- The client is satisfied that the extent of the scheme is known and desires that the prosecutor move quickly. The company engages a forensic accounting investigator with instructions to work with the prosecutor, thereby encouraging the

prosecutor to pursue the case expeditiously by taking advantage of the fact that the victim is offering and paying for expert assistance.
- The client's analysis of its fidelity bond or other insurance policies that may provide for recoveries determines that a prompt referral for prosecution is the best course of action.

Refer the Matter to State, Local, or Federal Prosecutors?

One of the interesting legal issues that may arise is the determination of what laws were violated. Clearly, if counsel determines that the referral should be to a federal prosecutor, a violation of federal law must be suspected. The forensic accounting investigator's findings as to the actual method by which the fraud or other type of crime was carried out may have a bearing on counsel's judgment. A case study will illustrate some of the issues.

A charitable organization was using a lockbox for the collection and processing of all of its contributions. One day a donor called to ask why a check she had mailed several months ago had not been cashed. Since the check had been for $10,000, the organization's administrators became alarmed. Soon they were receiving similar calls from other puzzled donors. After some investigation, the charity noticed a higher incidence of such occurrences at one of its lockbox locations. It notified its bank and local post office but could not determine the cause. Then a hotline tip came in that prompted the administrators to focus on a certain processing clerk at the bank. Law enforcement representatives followed the clerk home one day and, armed with a warrant, examined the clerk's property. They found a backpack and some trash that contained over 200 envelopes, complete with checks—all of them from donors.

What was going on? Overwhelmed with envelopes to process and unable to keep up, the clerk had not asked the supervisor for help but instead was taking unprocessed mail home and throwing it in the trash. A forensic accounting investigation soon estimated that over a period of nearly two years, the clerk had discarded more than $9 million in contributions! Not surprisingly, the leaders of both the charity and its bank were livid. They wanted to prosecute—especially because these amounts could never be recovered, as they had no idea whose contributions had been discarded.

The bank promised to make good on the defalcation, but its executives were anxious to prosecute and thereby send a message to all employees about ethical conduct. They took the case to the local U.S. attorney, who was interested in prosecuting the matter. The forensic accounting team had already done all the investigative work and developed an excellent evidence package. All parties prepared to move forward with federal prosecution of the clerk. But a little problem surfaced: The clerk had not violated any federal law. Because of not having cashed any of the checks and thereby gaining no financial benefit—except to have kept her job during that period—the clerk could be charged only with vandalism, which was a violation of a state, not a federal, statute.

Prosecutors Must Prioritize Cases

Should your client decide to go forward with a criminal referral, you should understand that while the federal government and state and local governments may differ in choosing which cases to prosecute, the principle that guides all of them is that

they are duty bound to protect the public from harm. The more harm they perceive, the more likely they are to pursue prosecution. A corollary principle is that prosecutors at all levels of government are resource constrained, and accordingly, you may discover that the referral of a white collar crime matter has to wait in line behind more pressing priorities—for example, other types of crime—say, terrorist activity, government corruption, or child pornography—or crimes of violence like rape and murder. As noted earlier, some citizens view white collar crimes as being victimless, but are they? White collar crimes can be devastating on a personal level when a company collapses and employees lose their savings, pensions, and jobs. Despite the significant personal impact, prosecutors nevertheless have many legitimate demands on their resources, and given this, focusing the attention of a prosecutor on a financial crime case may be difficult. Some forensic accounting groups include team members with experience as law enforcement agents—such as people from the U.S. Federal Bureau of Investigation—or with experience as prosecutors. These professionals can use their substantial experience to present the case in a manner that best deals with the prosecutor's concerns about resource limitations and complexity.

Regardless of the jurisdiction, however, the process may take as much as several years. If counsel is also advising a civil suit for recovery of losses, you may have to wait until the criminal matter is adjudicated before proceeding. Lastly, bear in mind that the authorities are not necessarily interested in determining your entire loss. They are not private investigators. They are looking only for sufficient evidence to satisfy the needs of a successful criminal prosecution. For example, say a controller has been stealing for several years by means of fraudulent invoices paid to bogus vendors. Furthermore, the prosecutor identifies $500,000 in theft over a one-year period. Do not be surprised if the prosecutor's investigation is concluded and the case prosecuted on this basis alone. The company may have unanswered questions: How long did this scheme go on? How much was stolen in total? Are there co-conspirators? Were there other schemes? These issues are relevant to the company, but not necessarily to the prosecution. Management may need to conduct an internal investigation to answer these questions.

Forensic Accounting Investigator May Increase the Success of a Referral

The forensic accounting investigator may become an important member of the prosecution team by helping assess evidence of financial wrongdoings and by advising the client and the prosecutor. Although not a lawyer and not in a position to offer legal advice, the forensic accounting investigator can point out weaknesses in the evidence and possibly suggest alternative investigative procedures to mitigate any risks that have been recognized. For example, if the CFO has set in motion an accounting scam, forensic accounting investigators can analyze financial statements and accounting transactions to determine what actually occurred. Many prosecutors do not have the in-house expertise to perform these steps. A forensic accounting investigator's expertise in gathering and interpreting financial evidence helps enable the prosecutor to strengthen the case and prepare to refute defenses.

Once a forensic accounting investigator is involved, it is important for that individual or team to conduct a very thorough investigation. For example, if the validity of the defenses offered by the suspect during admission-seeking interviews is

not tested, that may leave a weakness. The defense could use the weakness as a basis for portraying the forensic accounting investigator as an agent of the prosecution rather than an independent and objective witness. At a trial, there is an important distinction between a testifying forensic accounting investigator and, for example, a testifying psychologist. On one hand, the psychologist is considered an expert witness by virtue of testifying under the specific federal rules of evidence that govern expert-opinion testimony. On the other hand, the testifying forensic accounting investigator often is serving as a fact witness at a criminal trial: not generally offering an opinion but reporting the factual findings of the work. The forensic accounting investigator's task is to communicate the facts that that investigator has determined to be relevant to the matter at hand. While actual trial situations will differ depending on the circumstances, as a general matter it means the forensic accountant does not offer an opinion about fraud—as in, "Yes, in my opinion a fraud has been committed, and the defendant did it"—but, rather, presents evidence related to each of the elements of fraud in such a way that the trier of fact—in the form of judge or jury—may reach a conclusion based on the facts the forensic accountant has discovered.

Reputational Benefits

Reputational gains may also result from a referral. The company may be praised for standing up to fraudulent criminal activity and protecting other potential victims. Such a stand ultimately may have a positive impact on the company's bottom line or its stock price. The reaction of the market to the announcement of a prosecution against white collar crime is not wholly predictable, but taking a stand may enhance the company's reputation.

Employees are likely to be positively impressed if they see that management will not tolerate criminal activity, particularly in the managerial ranks. Furthermore, they will understand in very practical terms that the company's code of ethics is real and binding on all, and they probably will be more willing to come forward—to blow the whistle—if they see inappropriate activity in the workplace (see Chapter 8).

Customer and vendor relationships may also be enhanced if the company is perceived as taking a stand against financial wrongdoing. Both may feel more comfortable doing business with a trusted, reputable company.

The community also will be impressed. Public officials and community leaders admire companies that proactively take a stand against white collar crime. Note that the term *proactive* is chosen deliberately: Companies that appear to be merely *reacting* to external pressures may tarnish their reputations, while companies that communicate their active concern for values and the general welfare gain in reputation.

True, there also are risks to public disclosure of a significant fraud, such as adverse publicity. And therefore, an assessment of the amount and character of the publicity that may accompany a long public trial and the way in which the company should address that publicity is generally recommended. A public relations firm with a strong track record in this area should be engaged to determine the best way to deal with public perceptions of the company in the event of a trial.

In our view, the risks of adversely affecting a company's reputation through going to trial are outweighed by the possibility of enhancing a company's reputation through a firm and successful prosecution. A quote from Albert Einstein may

help guide a company faced with tough decisions: "In the middle of difficulty lies opportunity."

PLEA AGREEMENTS

Plea agreements are very common in white collar prosecutions and out of the control of the victim corporation. The defense will often realize early on that it cannot fight the documents. The defense attorney will attempt to minimize his client's possible jail time by putting the emphasis on mitigation at the time of sentencing. It is important to realize that even if a case pleads out, it does not mean the defense obtained a sweetheart deal. It usually means that the case was just too strong and the defense knew that a trial could result in more risk to the defendant. A strong forensic accounting investigator can help the prosecution achieve this type of result.

FILING A CIVIL LAWSUIT

It may be advantageous for the company to pursue a civil suit, especially in circumstances in which substantial financial recovery is possible. A company may file a civil suit at the same time as the prosecutor's pending criminal case, although discovery available under the civil statutes will often be stayed, at the request of the prosecutor, until after the criminal matter has been decided. A forensic accounting investigator can be of value in a civil case, especially in the process of discovering and presenting evidence. If counsel is pursuing civil litigation, the forensic investigator may well have access to sources of evidence through the discovery process not available in an internal investigation. For example, it may be possible to obtain additional documents such as the personal banking records and tax returns of suspects or to question suspects in a deposition under oath.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 20

Working with Attorneys

Thomas W. Golden, Michael T. Dyer, and Sonya Andreassen-Henderson

When matters arise at a company that require investigation, in-house or outside counsel often participate in or direct an investigation. The forensic accounting investigator often works with such counsel. That relationship is the subject of this chapter.

IN THE COMPANY OF LAWYERS

The first person to be contacted when there is a suspected fraud is often in-house counsel. Depending on the apparent severity of the matter and its apparent location in the company, other internal resources to be alerted at an early stage, in addition to the board, typically through its audit committee, may include corporate security, internal audit, risk or compliance management, the controller's office, and the public relations and investor relations groups. Investigations usually begin with extensive conversation about who should be involved, and the responsible executives may naturally wish to involve some or all of the functions just mentioned.

Depending on the circumstances, the group of internal auditors can in fact be a tremendous asset to an independent forensic investigative team. As participants in the larger team, internal auditors' knowledge of the company may improve both the efficiency with which evidence is gathered and the forensic team's effectiveness in lining up interviews and analyzing findings. Our advice to client executives and in-house counsel is to engage an external team but to consider making available to that team the company's internal auditors and other internal resources, after consideration for the needed level of independence, for any investigation of substantial size.

Forensic accounting investigators can expect to work with or for attorneys in a number of circumstances, including:

- Internal investigations with respect to accounting or reporting matters, generally triggered by:
  - Anonymous tips
  - Audit committee concerns
  - Internal audit concerns
  - External auditor findings
  - Regulatory inquiries

  - Media or regulatory reports or communications
- Regulatory investigations such as investigations by the U.S. Securities and Exchange Commission (SEC)
- Enforcement actions or inquiries from the U.S. Department of Justice (DOJ)
- Tax authority subpoenas or inquiries
- Civil litigation such as contract issues, shareholder lawsuits, wrongful-termination claims, and fraud recovery actions

The forensic accounting investigator may work with a variety of attorneys, such as the general counsel for the company; SEC or securities counsel; special independent (external) counsel to the board of directors or the audit committee, often referred to as 10A counsel;[1] attorneys for specific board or audit committee members; counsel for specific employees or groups of employees;[2] civil or criminal counsel; counsel for personnel who may be under suspicion or who hope to avoid that unwanted designation; and still others. The attorneys may be positioned as your client's adversary or your client's advocate, or they may be positioned as independent, as in the role of 10A counsel. It would not be at all unusual to have attorney representation of the following groups in a typical 10A investigation:

- The audit committee of the board of directors.
- The company, defending against a potential SEC enforcement action or a DOJ indictment.
- Officers or employees of the company, especially those named as subjects or targets of enforcement actions or investigations. Each could have separate counsel.

Each attorney serving a client in this roster generally has varying interests to protect, timetables to work against, and different views as to the significance of specific documents, interviews, and theories. The forensic accounting investigator should keep in mind these varying perspectives throughout the investigation so as to avoid unintentional sharing of privileged information, loss of confidential points of strategy, and the like.[3] While lawyers must adhere to ethical and legal guidelines, it is possible to communicate information accidentally, especially when working in physical proximity or with the same documents and personnel.

CONFIDENTIALITY REQUIREMENTS

A potentially material overstatement of asset values or revenues or understatement of liabilities or expenses is often the focus of investigation, and there may be an

[1] See fn. 6 in Chapter 5 regarding 10A and its reference to independent counsel, auditors, and other advisors.
[2] This is frequently the case for individuals who are expected to be interviewed.
[3] The issue of privilege is a matter best considered by counsel. The comments expressed in this chapter do not represent legal advice, and are based on the personal experiences of its authors, who are not attorneys. Privilege issues vary by jurisdiction and it would not be surprising to find differing views among equally competent counsel regarding what constitutes privileged material, or if privilege even exists. Seek competent legal counsel on this issue.

urgent need to inform stakeholders and markets that previously published financial statements may be unreliable. The extent of the problem should be determined and corrective action taken. In that scenario, a multitude of questions often swirl around the company: Was the misstatement deliberate? Who knew or should have known of the misstatement? What needs to be done? Who benefited?

In such investigations, confidentiality is usually very important. Leaks of information to the press or competitors may be particularly damaging. If the investigation is to be successful in uncovering the facts, the number of people within the company who are aware of day-to-day developments should be properly limited to avoid such leaks. The company may, however, voluntarily disclose information to regulators during such investigations. The forensic accounting investigator may on occasion become involved in an external investigation in support of various law enforcement or government organizations such as the SEC, the DOJ, the Federal Bureau of Investigation, the Internal Revenue Service (IRS), or even state or local prosecutors. This can come about in a variety of ways but typically occurs when the forensic accounting investigator's client has decided to refer the matter for prosecution and offers the forensic accounting investigator's assistance to the investigating agency. In such situations, attorneys for the government may find it useful to seek a 6(e) designation for the forensic accounting investigator. That designation grants the forensic accounting investigator access to grand jury or subpoenaed documents. Forensic accounting investigators do not have subpoena powers, but they can review documents obtained through subpoena if working under a 6(e) order. While access to such information can be very helpful to the investigation, a 6(e) designation may require some modifications to the investigation process, which should be discussed with the investigating team, including counsel. When retained in such instances, the forensic accounting investigator should have a thorough initial discussion with counsel and the government agency to ensure that the ground rules are understood and that the forensic team is fully aware of required modifications to the investigation process or methods. Later in this chapter, we return in more detail to the topic of working with law enforcement or government organizations.

FORMING THE INVESTIGATIVE TEAM

Forensic accounting investigators are frequently called upon to investigate potential financial statement manipulations or misstatements and asset misappropriations. For purposes of this discussion, we refer to such engagements as internal accounting investigations. When investigating asset misappropriation, the forensic accounting investigator may be engaged by the general counsel of a company or by the outside attorney who represents the company.

The forensic accounting investigator conducting an asset misappropriation investigation typically receives excellent cooperation from company executives, who perceive themselves and the company as the victim. Experience has shown, however, that an investigation focused on asset misappropriation may produce evidence suggesting other schemes in which the company may have been benefiting from illegal acts. Once the forensic accounting investigator picks up on a loose thread and follows it, it is difficult to predict where it might lead.

When potentially material accounting irregularities—or allegations of potentially material fraud—come to its attention, the board of directors typically seeks the advice of counsel on a number of considerations that may include the following:

- Identification of an independent committee—generally a subset of the board of directors and typically the audit committee—to lead the investigation and determine the company's approach[4]
- Initial communications with stakeholders, including employees, the market, stockholders, bondholders, lenders, and regulators
- Formation of an investigative team, generally through retention of appropriate counsel and other experts such as forensic accounting investigators and other specialists
- Urgent personnel decisions such as arranging for paid leave, restriction of duties or access, and termination
- Data preservation, stabilization, and security to avoid any loss of critical information
- Notification of insurance providers at the company and board levels
  The investigating team often includes:
  - Independent counsel
  - Forensic accounting investigators
  - Forensic technology experts
  - Subject matter specialists
- Based on the specifics of the investigation, the team may include other experts or specialists such as:
  - Engineers
  - Actuaries
  - Tax experts
  - Investment bankers
  - Valuation or appraisal specialists
  - Damages experts

How involved will the attorney be in the planning and execution of the investigation? On one hand, the forensic accounting investigator may find that the attorney gives the forensic accounting investigator free rein to devise and execute a strategic investigative plan, subject to the attorney's approval. That scenario is particularly likely in cases of asset misappropriation. On the other hand, some attorneys insist on being involved in all phases of the investigation. It is the attorney's call. When engaged by counsel, forensic accounting investigators take direction from counsel.

[4] It is important to recognize that it is the responsibility of the company, typically through its board of directors, to conduct a thorough investigation, especially in any matter that may be material to the financial statements. Whatever authority the forensic accountant has in the conduct of the investigation, it is not the forensic accountant's investigation; it is the company's. This does not, however, release forensic accountants from the ethical obligations and rules required by their professional associations, such as the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

They should advise according to their best judgment, but in the end they work at counsel's direction.

Forensic accounting investigators bring a special skill set, perspective, and experience to the internal accounting investigation, complementary to the skills of auditors, counsel, and other experts typically involved in these investigations. Capable forensic accounting investigators can be found within most large accounting firms as well as in boutique, or specialist, firms. Whether approached by counsel or directly by the company to participate in an internal accounting investigation, forensic accounting investigators should immediately assess their independence (see Chapter 11 and a later section of this chapter). Once independence has been determined and forensic accounting investigators have been retained, those investigators should obtain a thorough understanding of the respective roles and responsibilities of the various team members to allow for efficient and effective coordination across the team. Failure to clearly establish and fulfill roles and responsibilities may lead to wasted time and money—or worse, to gaps in the investigation process and incomplete or inaccurate results. These shortcomings may reduce the value of the investigation and may even subject the company and its officers and directors to adverse publicity or liability.

While it usually is easy enough in theory to delineate the team members' responsibilities and to set up procedures that ensure communication across the team, it often is much more difficult to accomplish those things during the stress and urgency of an investigation. Forensic investigations are often conducted in a crisis atmosphere that disturbs communication and allows duplication in the investigative process to slip through. In spite of deadline pressure and extensive work to be performed, time must be found to coordinate and share the information being obtained. When working with attorneys, forensic accounting investigators should specifically understand:

- Their expected role and responsibilities vis-à-vis other team members
- What other professionals are involved (current or contemplated)
- The extent and source of any external scrutiny (SEC, IRS, DOJ, and so on)
- Any legal considerations (extent of privilege, expectation that the company intends to waive privilege, expectation of criminal charges, and so on)
- Anticipated timing issues, if any
- Expected form, timing, and audience of interim or final deliverables
- Specifics of the matters under investigation, as currently understood by counsel
- Location of and steps taken to identify and preserve potentially relevant data
- Any limitations on departments or personnel that can be involved, interviewed, or used in the investigation process

As noted at the beginning of this chapter, prudent forensic accounting investigators typically perform their assignment under the presumption that any deliverables, work product, or work process may become publicly available or accessed and used in civil or criminal litigation proceedings. That being said, when a company employs an attorney to represent it, the attorney's work product usually cannot be subpoenaed. Attorneys enjoy a number of privileges that are necessary to ensure that their client can be completely honest with them without fear of disclosure. The forensic accounting investigator who is employed directly by the attorney is considered an extension of the attorney, and the forensic accounting investigator's work product

may be protected from subpoena, unless the adverse party in litigation can prove, among other things, that there has been a "waiver of the privilege." If work product or other privileged information is intentionally shared with individuals outside the privileged group, the privilege may be lost.

The forensic accounting investigator should be careful to protect the privilege and should mark each and every individual document prepared with the caption "privileged and confidential—attorney work product" or words to that effect. This caption serves as a reminder and notice that the documents are privileged and not subject to subpoena or discovery. In practice, it is true that the privilege may be waived by the company and that the forensic accounting investigator's spreadsheets, documents, and other working papers, as well as testimony, will be volunteered or subject to subpoena. It should also be understood that privilege is a jurisdictional issue and decisions can fall either way. When privilege is contemplated, however, it is still good practice to mark all documents with the privilege disclosure, so that they can be readily identified as privileged in the future. It also makes it easy to determine documents prepared by the forensic accounting investigator as opposed to ones prepared by client staff.

Independent counsel, with the help of forensic accounting investigators, often takes the lead in setting up, organizing, and managing the investigative team and process. This may include the selection and retention of other parties who make up the team. Independent counsel's responsibilities typically encompass the following:

- Preparing, maintaining, and disseminating a working group list (very helpful in sorting out which law firms or experts represent whom)
- Establishing the timetable in conjunction with the board of directors or management, disseminating the timetable to the investigating team, and tracking progress against it
- Compiling, submitting, and tracking the various document and personnel access requests that the investigating team members will generate
- Organizing client or team meetings and agendas
- Preparing the final report with or for the board or its special committee, or doing so in conjunction with other teams from which reports are forthcoming
- Establishing and maintaining communication channels with the board of directors and other interested parties, generally including internal general counsel, company management, regulatory personnel, law enforcement or tax authority personnel, and various other attorneys involved

Although the attorney may lead the investigation formally, the forensic accounting investigator frequently is the cornerstone of a successful investigating team. The forensic accounting investigator may provide the following types of assistance and support for the larger team directed by the attorney:

- Ability to plan and conduct a proper financial crime investigation
- Expertise in accounting, regulatory requirements (such as SEC) auditing, internal controls, and financial analysis
- Interviewing skills, both fact-finding from witnesses and admission-seeking from targets
- Expertise in performing data mining and data interrogation of the company's books and records, including e-mail and other electronic records

- Experience in document authentication and knowledge of a network of subspecialists trained in highly technical authentication procedures such as typewriter or printer analysis and authentication through forensic laboratory science
- Ability to review and interpret internal accounting transactions and their compliance with various rules
- Ability to accumulate public financial and nonfinancial information, including SEC or company registry filings, if applicable
- Forensic imaging and other information technology (IT) expertise such as e-mail search tools
- Support of counsel in developing various hypotheses and investigative procedures and techniques
- Background checks on relevant personnel
- Vendor validity checks on the basis of publicly available information
- Preparation of specific sections of the draft and final reports or support of counsel for report sections that focus on accounting, reporting, or financial information
- Coordination with both internal and external auditors and the audit committee
- Review and critique of financial, accounting, or reporting analysis and advice provided by other specialists
- Among larger firms, a global network of investigators to assist in multinational investigations

Particularly when investigations include review and analysis of accounting and financial information, the forensic accounting investigator is often a critical member of the team. Some attorneys do not have extensive accounting or auditing experience, and certain accounting concepts may be foreign to them. In a recent investigation, counsel contacted the forensic accounting investigators as the final draft of the report was being prepared because counsel was uncertain about the concept of a "reserve"—its significance and how to explain it in the report. The forensic team gave an instant tutorial on how reserves can be manipulated and then helped draft the relevant section. In another instance, counsel coordinated interview schedules with the forensic accounting team to ensure that an experienced SEC accounting specialist was available to participate with counsel in the interview of the company's controller and chief financial officer (CFO). The SEC specialist's participation turned out to be critical because the interview agenda included discussion of the adoption of two new accounting rules as well as discussion of the extent to which the external auditor was familiar with the new rules.

Forensic accounting investigators are frequently conversant in areas related to financial accounting and reporting such as valuation, tax, and financial aspects of human resource management, but "conversant" does not necessarily indicate a sufficient level of knowledge to guide a complex investigation. For complex investigations or investigations that involve public companies, it is often wise for the lead forensic accounting investigator to assemble a team that includes the following skills and experience:

- Ability to conduct or assist with the investigation
- Knowledge with respect to Generally Accepted Accounting Principles relevant to the applicable time period of the investigation
- Knowledge with respect to SEC-compliant accounting, financial disclosure, and other reporting

- Familiarity with the regulatory investigative process
- Knowledge with respect to Generally Accepted Auditing Standards and procedures
- Ability to immediately access industry or specialist knowledge as required—for example, expertise in derivative financial instruments, bank regulation requirements, and long-term contract accounting
- Familiarity with the uses and abuses of offshore companies and trusts
- Ability to identify departures from customary commercial behavior and business practices
- Relevant language skills and ability to meet the challenges of a geographically diverse investigation, as required

Each of the foregoing skills represents an area in which independent counsel frequently requires guidance and support by the forensic accounting investigator.

While forensic accounting investigators are often critical components of an effective internal accounting investigation, it is important to remember that they are engaged as fact finders. Forensic accounting investigators may need to educate or remind counsel about the limitations of the forensic accounting investigator's expertise and scope of service. In particular, the forensic accounting investigator should take care to avoid:

- Providing legal advice or making legal assertions in their work or deliverables.
- Providing actuarial or valuation guidance unless appropriately credentialed and trained.
- Acting as a judge or jury by making judgments as to the guilt or innocence of particular people or groups.
- Expressing an audit opinion on financial statements or internal control effectiveness. Note, however, that commenting on specific elements of financial statements is entirely appropriate and can be legitimately expected of forensic accounting investigators with accounting and auditing experience.[5]
- Creating legal exposure as a result of comments that may lead to claims of defamation, libel, slander, and the like.

On occasion, the forensic accounting investigator may need to remind staff, other parties, and counsel of those limitations.

The board or special committee of the board, in conjunction with counsel, frequently issues a written report following an internal investigation, especially if the focus of investigation is a public company. The report may include work performed or evidence reviewed by the forensic accounting investigator, sometimes with an explicit reference to the forensic accounting investigator. For example, a report of the Special Investigative Committee of the Board of Directors of Enron Corporation, prepared by counsel, exceeded 200 pages and specifically referred to a major accounting firm that had been engaged to provide accounting advice. Likewise, both the Report

[5] As discussed earlier in the book, it would be wrong to assume that all forensic accountants have accounting, auditing, or SEC regulatory experience. Extensive interviews of potential financial experts are critical to assembling the right investigative team.

of Investigation by the Special Investigative Committee of the Board of Directors of WorldCom, Inc. and the Examiners Report on the Lehman Brothers Holdings Inc. bankruptcy reference accounting or financial advisors. In other instances, the various experts involved in an investigation issue separate, stand-alone reports. As previously mentioned, the forensic accounting investigator should discuss the form, timing, and audience of all final deliverables early in the process to avoid confusion, unnecessary work, or misunderstandings.

DOCUMENTATION

Owing to the presumption that an internal investigation may result in or ultimately contribute to litigation, appropriate documentation practices are critical. Generally, the documents reviewed by the forensic accounting investigator in both print and electronic formats will come from the following sources.

- Public information, including SEC filings, press releases, analyst reports, background checks, and Internet searches
- Documents provided by the company—voluntarily, for most internal investigations
- Legal documents and filings available to counsel
- Accounting records provided by the company
- Information from the external auditor

Information critical to forming conclusions that support remedial actions may also emerge from interviews with key company personnel and possibly other parties.

Document volume and complexity will be driven in large part by the scope and duration of the investigation. Regardless of the volume, it is incumbent upon the investigating team to track, organize, disseminate, and control the documents. Counsel often assumes primary responsibility for document management and gives instructions to other team members. Counsel may establish an indexing process by Bates numbers, may establish imaging or warehouse storage, and may assume primary responsibility for providing for all relevant members of the team the documents and data files obtained. It is important for the forensic accounting investigator to conform to these practices. Proper communication at the outset may prevent misunderstandings.

Although many documents and data files typically will be provided directly for counsel by company personnel, forensic accounting investigators are likely to receive many financial, accounting, or reporting documents and data files directly from company personnel. The forensic accounting investigator should establish procedures for sharing any such documents with the rest of the investigative team and for accurately cataloguing and tracking them according to source, date received, investigation topic, and so forth. This approach often is especially useful when the time comes to write the report or to respond to questions after the fact. Consistent with the process used in an external audit, the forensic accounting investigator should prepare and retain sufficient documentation to support any reports, memorandums, or other deliverables issued. When documents are to be presented to third parties, duplicate copies

are essential: one for distribution as requested, one for counsel, and one for the forensic accounting investigator's records. It is not enough simply to make a note as to what documents have been issued. Avoid all possible confusion by making a copy of the document supplied and filing it separately. This system is especially helpful when the investigative team is preparing for depositions or trial and has to know exactly what documents and files are in the opposing lawyer's possession. It takes extra time to follow this procedure, and it creates a much larger document cache, but the effort is well worthwhile. As noted in a previous chapter, we encourage early discussion with counsel regarding document retention.

CIVIL LITIGATION

If civil litigation involving individuals is ongoing, the investigating team can use the discovery process to gain access to various types of personal information from the charged individuals not typically available to the team in the normal course of most investigations, including:

- Financial records
- Bank statements and account information
- Tax returns
- Asset ownership details
- Purchase, sale, and investment documentation
- Travel records or other data of interest to the investigation

It is extremely helpful in many investigations to learn whether the target has sources of income that cannot be explained. How to go about this? Courteously asking the individual to produce bank statements is usually unlikely to result in the individual's compliance with the request, and from a strategic perspective, you will have tipped off the target that an investigation is under way. The target may also decide to document for you only accounts that show benign and perfectly normal transactions or provide altered documentation.

INTERVIEWING

While this topic is covered extensively in Chapter 16, a few points should be summarized here about working with attorneys. It is not an uncommon practice for the investigating team to conduct a large number of interviews. Interviewing is a valuable tool in understanding an organization and individual roles, responsibilities, and perspectives. Interviews may extend beyond company personnel to include suppliers, customers, legal counsel, business partners, ex-employees, and still others.

When the investigation includes accounting issues, interviews typically encompass accounting and reporting personnel, management with responsibilities for the financial statements, the internal audit department, audit committee members and staff, external auditors, and perhaps others. The background and expertise of the forensic accounting investigator often are well suited to support counsel during these

interviews. Unlike external investigations conducted by the SEC, DOJ, or IRS, internal investigations face a number of limitations, including:

- *Lack of subpoena power.* Interviews are voluntary, and the person being interviewed can walk away at any time.
- *Testimony not under oath.* The individuals being interviewed are not under oath to tell the truth, but lying to the forensic accountant may trigger liability under statutes that preclude such conduct.
- *Interviews that are more informal than depositions.* The output consists simply of interview notes taken by counsel or others participating.
- *Interviews that rely on the cooperation and availability of the interviewee.* Continuing employment is usually enough of a motivator to compel an employee interviewee to talk with you; it is more difficult, however, to persuade nonemployees to be interviewed.

EXTERNAL AUDIT FIRM

Before accepting a forensic accounting investigation engagement, the forensic accounting investigator should assess whether there are independence issues that disallow acceptance of the engagement or limit its scope. Although this topic is discussed in detail in Chapter 11, it is worthwhile to summarize the general guidelines here.

While it is true that one of the goals of the Sarbanes-Oxley Act is to mitigate independence concerns by identifying services that the external auditing firm is precluded from performing for audit clients, Congress did not want to restrict audit committees from engaging those professionals that such committees regard as fully competent to perform investigations into allegations of financial improprieties. It may be entirely appropriate to engage forensic accounting investigators from the company's external audit firm in some but not all situations. The decision to use or to refrain from using the external auditor firm to investigate allegations of fraud usually depends on several key factors, discussed later. When an audit committee is made aware of indicia of fraud or even the slightest suspicion of fraud, it usually wants answers fast. Assembling a competent investigative team to fulfill the board's responsibilities as quickly as possible is generally a high priority. In some cases, the quickest way to find valid answers to the questions asked by the company's directors is to bring in forensic accounting specialists from the external audit firm. Are the allegations true? And if they are true:

- What are the financial accounting or reporting implications?
- Who is involved in the alleged improper act?
- How significant and pervasive is it?
- How did it occur and go undetected until this time?
- What actions need to be taken to remediate the system of internal controls so that this does not happen again?
- Are we vulnerable in any other areas?

Those who would argue for a forensic accounting team from a firm other than the external auditors do so for reasons other than Sarbanes-Oxley, because

Sarbanes-Oxley specifically allows for this. There may be a belief that the auditing firm cannot be independent; it has already been established, however, that the external public auditing firm is independent: Under no other circumstances could it perform the audit. There may be a belief that engaging the external audit firm would generate a conflict of interest. This may in fact be a valid concern—for reasons explored in Chapter 11. If there is a conflict, the appearance of objectivity may be impaired. When there is a concern that the allegation may lead to a potential restatement of the financial statements, a conflict of interest is entirely possible. In that case, a forensic team independent of the external auditor would need to be retained—probably by counsel.

During a 10A investigation, counsel may be assisted by an independent forensic team. It is possible that the audit firm will deploy its own group of forensic accounting investigators in a specialist role, consulting with the audit team. The group will shadow the investigation conducted by company's counsel to aid in bringing the investigation expeditiously to completion. This is not to imply that the audit team should in any way instruct the 10A investigative team on procedures that should be performed. It is the audit committee's investigation. However, close and timely communication between the investigative team and the auditors is a good way to ensure that all parties, including the auditors, are comfortable that the investigation was conducted in an appropriate fashion and that findings were communicated to the auditors in time for them to react to the findings appropriately. Without this level of cooperation, the auditors would not know of the investigative team's findings until those findings were communicated by the investigative team to the audit committee, and the auditors could not therefore begin their independent review of the support or bases for conclusions reached until after that communication. Alternatively, audit committees may retain a forensic accounting team from the company's auditing firm to investigate, provided—as prescribed by SEC rules—that no regulatory proceeding or investigation has been initiated.

Under both scenarios (the audit firm's forensic team is engaged or the audit firm shadows a forensic team engaged from another firm), the auditor is more than likely to require attorneys leading the investigation (10A counsel), on behalf of the company, to disclose the investigative findings and supporting evidence. The auditor will be well-advised to inform the audit committee and its counsel in advance that the auditor needs to be kept fully informed. Notifying in this way may avoid difficulties at the conclusion of the investigation, which could delay the timely filing of SEC reports.

If a formal proceeding is initiated or the company is notified that it is the subject or target of an investigation by an enforcement agency such as the DOJ, the company should consider engaging a forensic accounting team independent of the auditing firm. It is still likely that the audit firm's forensic accounting investigators will shadow the investigation for reasons mentioned earlier. The findings of that shadow team may be shared with the company and its counsel. Duplication of efforts may be avoided or at least somewhat mitigated in this manner. For example, e-mails can be reviewed by the forensic team from the auditing firm and findings communicated to 10A or other counsel at the company's direction. However, certain limitations would need to be well understood and respected. The auditing firm may not, for example, provide litigation support, a service specifically precluded by the Sarbanes-Oxley Act when a regulatory proceeding is under way.

Most auditing firms take the view that counsel appointed to conduct a 10A investigation must be independent of the company. This requirement does not mean that counsel is not permitted to have ever worked for the company before, but attorneys playing this role cannot be drawn from the company's law firm of choice for prior litigation. Similarly, while knowing that it will shortly act as an advocate for the company in any enforcement action, 10A counsel cannot be expected to render an objective opinion on the possibility that an illegal act has been committed. Also, a forensic accounting team selected to support the company's legal defense must likewise be independent of the forensic accounting team that assists 10A counsel. These are obviously intricate issues—with extended implications concerning who can do what while remaining strictly within regulatory guidelines.

It is possible to make available certain of the auditor's working papers to the forensic accounting investigators assisting either 10A counsel or the company's defense counsel. This may be accomplished through execution of an access letter, if the auditors are willing to voluntarily cooperate.

Before permitting access to the working papers, the incumbent accountant may wish to obtain a written communication from the firm providing forensic accounting investigative assistance regarding the use of the working papers. These letters are not required by professional standards but certainly make good business sense. Why give voluntary access to a party that may later use what it finds as a basis to bring a claim against you?

Even with the client's consent, access to the incumbent accountant's working papers may still be limited. Experience has shown that the incumbent accountant may be willing to grant broader access if given additional assurance concerning the use of the working papers. Accordingly, the forensic accountant might consider agreeing to the following limitations on the review of the incumbent accountant's working papers in exchange for broader access:

> *Because your review of our working papers is undertaken solely for the purpose described above and may not entail a review of all of our working papers, you agree that (1) the information obtained from the review will not be used by you for any other purpose; (2) you will not comment, orally or in writing, to anyone as a result of that review about whether our engagement was performed in accordance with Statements on Auditing Standards; (3) you will not provide expert testimony or litigation services or otherwise accept an engagement to comment on issues related to the quality of our engagement.*[6]

Such letters will likely enable the recipients to review by sight only selected working papers. The access letters should restrict the use of the information and prevent both counsel and the independent forensic accounting team from assisting the company in any action against the audit firm.

---

[6] American Institute of Certified Public Accountants, www.aicpa.org/download/members/div/auditstd/Illustrative_Successor_Accountant_Acknowledgment_Letter.pdf.

WORKING FOR OR INTERACTING WITH LAW ENFORCEMENT OR GOVERNMENT AGENCIES

In the course of a forensic accounting investigation, the forensic accounting investigator often encounters law enforcement agents and prosecutors. Both will inevitably ask for information concerning the progress or results of the forensic accounting investigation. The forensic accounting investigator should determine from the client—and often, client's counsel—what information the client wishes to turn over voluntarily. The client may decide it is advantageous to assist the prosecutor and may wish forensic accounting investigators to assist the prosecutor by turning over the results of their investigation, sharing information, or conducting additional investigation procedures as requested by the prosecutor. However, investigation processes often become more complex if the prosecutor makes grand jury material available to forensic accounting investigators for review.

Grand jury rules vary depending on whether it is a state or federal grand jury, but there are broad similarities. The grand jury conducts an investigation to determine whether there is sufficient evidence to indict. The prosecutor drafts an indictment, and the grand jury votes as to whether the evidence reviewed is adequate to support the indictment. Grand jury materials and information are confidential, and criminal and civil penalties are imposed for grand jury secrecy violations. However, the prosecutor may turn over subpoenaed information to authorized individuals, including law enforcement. Grand jury material may be shared with other individuals in some circumstances to facilitate obtaining information that furthers its investigation. Normally, an administrative process lists everyone who is authorized to access grand jury material. That list is detailed and precise, and only those listed are granted access.

If the prosecutor has requested that the forensic accounting investigator review documents obtained by the grand jury and if the client has agreed to such an arrangement, an interesting situation is created. The client is paying the fees of the forensic accounting investigator, but the forensic accounting investigator will in most instances be barred from giving any of the new information to the client. The client must be content that assisting the prosecutor corresponds to also assisting itself, even though that client will have no knowledge of the information to which the forensic accounting investigator now has access. When authorized to work with grand jury material, the forensic accounting investigator must make sure that the client understands the restrictions. The forensic accounting investigator must also discuss in detail with the prosecutor how to ensure that there be no violation of the rules of access and keep an open line of communication with the prosecutor for inquiries as to whether said accountant's actions fit within the rules.

In some instances, state and federal prosecutors have hired forensic accounting investigators to conduct entire investigations, generally in situations in which the available law enforcement officers do not have the requisite resources. In such instances, the forensic accounting investigators' involvement with the grand jury may be extensive and ongoing, and those investigators will be exposed to the full range of rules governing grand jury procedures and documents: the access rights of outsiders, the rights of subjects under interview, chain-of-evidence requirements, and the like. The forensic accounting investigators should work very closely with the prosecutor throughout the investigation and fully understand the rules and guidelines in advance.

DISAGREEMENTS WITH COUNSEL

Disagreements with counsel will arise from time to time when forensic accounting investigators are shadowing a 10A investigation. They are advising the auditors as to the conduct of the investigation and likely sufficiency to satisfy the auditor's responsibilities under Section 10A of the Exchange Act. Such differences usually focus on the scope and strategy of the investigation. The authors have been fortunate to work with many bright, experienced, and informed attorneys who conduct their investigations with the expert skill and proper independent mind-set required of professionals charged with the responsibility of determining all the facts. On occasion, however, we have also found ourselves working with attorneys who are inexperienced at serving as independent 10A counsel, falling back instead on their more familiar role as client advocates playing the defense counsel role. In such situations, it is always best to try to work out your differences with counsel. Forensic accounting investigators who find they still have issues after a strenuous good-faith effort to resolve differences need to bring those differences to the attention of the directors charged with oversight of the investigation—usually, a special committee of the independent directors of the audit committee.

A recent SEC action has brought to the forefront the commission's concerns about the conduct of some investigations. Former SEC enforcement director Stephen Cutler said in a September 20, 2004, speech that he is "concerned" that some lawyers hired to conduct financial crime investigations might actually have helped "hide ongoing fraud, or may have taken actions to actively obstruct such investigations."

Judging by threatened enforcement actions and other communications, it appears the SEC is reviewing the quality and robustness of investigations, in which most decisions about procedures to perform and whom to interview are under the judgment of the lawyers charged with conducting the investigation. There will no doubt be more to come on this issue, but early signs from the SEC should serve as warnings to lawyers that they should conduct financial crime investigations in a rigorous and robust fashion as an expected part of doing their job. The issue of the quality of investigation will continue to evolve, as evidenced by the SEC's notification to a lawyer that he may face civil sanctions for his role in an investigation at a medical device maker in Irvine, California. The unusual action of the SEC suing a lawyer over allegedly mishandling a corporate probe sends the message to lawyers that they must choose between serving as defense counsel and conducting a thorough investigation as independent professionals responsible to the board or audit committee, which serves investors' interests.

Here are some examples to illustrate our point about selecting appropriate investigative procedures and executing them well.

- *Gathering electronic evidence:* Either electronic evidence should ideally be gathered by the forensic accounting firm's own IT specialists or those specialists should closely supervise the company's IT personnel. Also, in some cases, forensic images should be made of hard drives and the like instead of merely copying them. And it is best to be more, rather than less, aggressive in choosing the number of personnel whose electronic data you select to examine. For example, the hard drive of a controller who has been accused by a whistle-blower

of manipulating earnings is an urgent subject of forensic examination. It might be prudent to image the hard drives and examine the e-mail of some of those reporting to that controller as well as the controller's administrative assistant.

- *Interviewing:* Chapter 16 explores this complex investigative procedure in depth. The complexity of the interviewing procedure is not always understood or respected. For example, we have seen certain lawyers approach interviewing as a simple note-taking exercise: Put the documents in front of the subject, and write down what the subject says in response. That is clearly the wrong way to conduct an interview in these matters. Imagine you have discovered an e-mail in which the CFO writes, "Don't tell the auditors about this transaction." Before showing this e-mail to the CFO, you would want to probe the subject through questioning: "Have you ever instructed anyone to withhold information from the auditors?" This would be just one of many questions you would ask. You want to nail this issue down *before* producing the e-mail. Yet some lawyers would begin the interview by simply handing over the e-mail and asking the CFO to explain it. That gives the CFO ample time to come up with some inane explanation for making the comment.

Consider another example. A shipping clerk says in a preliminary interview that the supervisor said to record the goods as shipped, even though the goods were still on the dock. To get to the bottom of the matter, the lawyer decides to interview both the clerk and the supervisor together. Not surprisingly, the shipping clerk now changes his story to agree with the supervisor's. The two should have been interviewed separately and instructed not to discuss the matter with anyone.

In situations in which you believe the lawyers are not conducting a robust enough investigation, it is wise to take your concerns directly to those charged with oversight of the investigation. It is ultimately their responsibility to ensure a thorough and proper investigation.

CONCLUSION

The forensic accounting investigator can expect to work with or for attorneys in most investigations. To help ensure that the investigation progresses as smoothly as possible and reach appropriate conclusions and satisfactory resolutions, each member of the investigating team should:

- Work collaboratively within the investigative team assembled by the client: Frequent conference calls are likely to facilitate this objective.
- Communicate early and often with the team: When disagreements arise as to approach, which is not uncommon, discuss them immediately and thoroughly to reach a mutual understanding.
- Demonstrate respect and recognize the distinct expertise of the various investigative team members: Both counsel and the forensic accounting investigator have unique skill sets that may be critical to the success of the investigation. Egos should not get in the way of serving the client.
- Foster a professional, cooperative environment: "We have a job to do. Let's work together to get it done."

- Acknowledge and manage the typically high pressure environment and the likelihood of external scrutiny.
- Understand the rules of the game in regard to documentation and reporting expectations, other parties involved, expected level of assistance from the company, 6(e) restrictions, Section 10A requirements, and so on.
- Have clearly understood roles and delineated responsibilities in an effort to minimize both duplication and gaps in the investigation process.

Generally speaking, qualified forensic accounting investigators and attorneys work well together. Many engagements end with the appreciative recognition among all team participants that cooperation and a mix of highly professional skills brought clarity and resolution. Internal accounting investigations can be performed most efficiently and effectively when the attorneys and forensic accountants acknowledge and respect the expertise that each brings to the matter—fulfilling the roles best suited to their expertise.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 21

Financial Reporting Fraud and the Capital Markets

Daniel V. Dooley and Steven L. Skalak

The world's major capital markets are informed and fueled by accurate, complete, and timely financial information of all types. While other types of information—commercial, scientific, political, weather, and demographic data—are also relevant to capital market activity, no other kind of information is as sought or as relied on in the normal course of the capital markets' operations as is financial information. This is so whether you define *capital market* as individual investors trading a company's shares on a stock exchange or as sophisticated private equity firms investing in emerging companies. In fact, to discuss fraud comprehensively, a relatively broad definition of capital markets should include all forums in which consumers of capital contract with suppliers of capital to fulfill their requirements. Wherever money is involved, that is where you will likely find the fraudsters.

There are many types of capital markets. They include both debt and equity markets for the issuance of publicly traded securities, implemented by organized exchanges and also by special types of markets, as in the case of certain debt instruments such as U.S. Treasury securities. Similarly important are credit markets, in which companies, governments, and individuals can borrow funds for both short- and long-term use from lenders ranging from traditional banks and commercial paper markets to credit card issuers. Also figuring in this inventory are organized exchange markets such as the commodities exchanges in Chicago and London; the Chicago Board of Trade, where agricultural commodities are traded; and the London Metal Exchange, where both base and precious metals are traded. Managed investment funds ranging from public mutual fund complexes to private hedge funds open to only a few selected investors also represent an important sector of the capital markets. Foreign exchange markets must be considered: Billions of dollars of currencies are traded every day in spot and forward markets around the world. Finally, the secondary markets—in which individuals and the world's largest investors, such as pension and mutual funds, trade in the debt and equity securities of public companies—must be included.

Participants in all of these markets rely on financial information of one type or another to direct the flow of their funds and determine their trading strategies. At the most fundamental level, capital markets are about the flow of money from one party

to another, and to a fraudster they represent an opportunity to redirect the flow of funds, often by deceiving transaction parties with false financial information.

TARGETS OF CAPITAL MARKET FRAUD

Experience has shown that anyone in a position to lend money to or invest money in the business venture of another is likely at some point to be the target or—as the fraudster hopes—the victim of fraud. All capital market participants can be victimized in one way or another; none are exempt. For example, banks can be duped into making loans to fraudulent enterprises, or by becoming indirect participants in fraudulent schemes such as money-laundering operations in which the services of the bank are used for improper purposes.

The primary participants in the capital markets are:

- Banks, including commercial banks, money center banks, national or central banks, savings and loans, credit unions, and mortgage bankers
- Investment banks—the primary underwriters of newly issued securities in both the debt and equity markets
- Broker-dealers—that is, stock and bond brokers for both institutional and retail (individual) customers, foreign exchange traders, primary dealers in U.S. Treasury securities, online or Internet stockbrokers, and commodities brokers and traders
- Insurance companies
- Mutual funds and their advisors and sponsors
- Individual investors

Excluding individual investors for the moment, all of the other participants may become victims of fraudulent schemes in three fundamental ways: by being attacked from within, generally by a rogue employee exceeding the scope of his authority for personal gain; attacked from the outside through a wide variety of schemes to obtain funds under false pretenses; or used as an unwitting participant to facilitate a fraudulent scheme perpetrated on others or for the benefit of others. Money laundering is the classic example of the third category.

Some simple examples of the first two categories would be the loan officer who approves bogus loan applications and disburses the money to entities he secretly controls and the currency, bond, or commodities trader who hides losses and then tries to trade his way out of the losses through transactions that exceed approved limits.

Financial institutions such as broker-dealers in securities, commodities brokers, investment banks, investment management firms, and mutual fund complexes can also perpetrate fraud. Generally, this occurs when institutions use for their own advantage their greater access to key information about investment values and prospects instead of sharing the information with their clients. In the dotcom bubble of the 1990s, many investment banking houses earned lucrative fees for bringing new stock and bond issues to market for corporate giants like Enron and WorldCom, as well as for untried dotcom initial public offerings (IPOs). This activity was supported in part by their analysts pumping out research reports touting the companies' stock.

Only after the fact did investors learn of internal e-mails showing that the analysts and investment bankers had long before concluded that the business prospects of these companies—clients of the banks—were not at all as rosy as their reports had portrayed.

The recent real estate bubble in residential housing prices in the United States is another example. During the last decade, many financial market participants sold mortgage loan products to individuals that promised low payments initially but in exchange for the risk of readjustment to higher payments later. Borrowers were frequently encouraged to rely on the seemingly unending upward spiral in home values to take on such products because they could always refinance their mortgages based on higher future values. Of course, the fundamental flaw in this logic was the expectation of constantly rising home values, with the consequence that when values fell and the initially low payments adjusted upward, thousands of home owners struggled to make payments, creating a liquidity crisis of global proportions.

This is the latest revival of the long-running melodrama "Wall Street versus Main Street." The state of Kansas, in 1911, initiated the blue sky laws, later emulated by many other states. There followed in later decades the Depression-era revolution in investor protection and market regulation with establishment of the U.S. Securities and Exchange Commission (SEC) in 1934; the Investment Company Act of 1940; and the Security Investors Protection Corporation, initiated in 1970, which introduced stringent rules covering suitability, churning, time stamping, trade reporting, and program trading. There has also been vigorous litigation concerning the use of derivative instruments by Gibson Greetings and Procter and Gamble, imposition of the fair disclosure regulations, and the Sarbanes-Oxley Act of 2002. Most recently, in response to the credit crisis of 2008 and 2009, an entirely new Bureau of Consumer Financial Protection has been created by Congress. This will substantially alter the manner in which consumer interests are represented in the regulatory environment.[1]

Although this body of legislation, institutions, and rules is powerful, sophisticated insiders have occasionally taken advantage of less-informed investors since the dawn of modern capitalism. Nonetheless, the model of securities investing based on financial information is a central feature of modern economies, and the task of all ethical participants in the corporate reporting supply chain is to do all they can to ensure that the information is reliable, complete, clear, and timely.

SECURITIES INVESTMENT MODEL

Investors purchase equity securities in the expectation that their investments will generate a satisfactory return in at least one of two ways—or, ideally, in both ways: through dividends and through appreciation in the market value of the securities. Market value can be influenced by many factors, but for the most part, the value of equity securities is based on the profitability of the enterprise. Value may be measured and predicted by consideration of past (that is, historical) performance, by assessment of the current results of operations and financial condition, and by evaluation of

[1] See Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

likely future results. Some of the metrics of corporate performance—past, present, and future—are accounting measures, such as:

- Revenues and revenue trends
- Profit margins
- Earnings and earnings trends
- Cash flows from operations and expected future cash flows

Other indicators of potential value may include known or anticipated market success of existing or anticipated products and services; market share; competitive factors such as intellectual property rights, management quality, customer base, superior distribution, or effectiveness of supply chain and manufacturing resources; and technological advantage. These value indicators are proxies for operating results, in that they are expected to result in increased value of equity securities because of their inherent ability to create revenue growth, control costs and expenses, achieve attractive profit margins, and, ultimately, obtain increased profitability.

Risk is a factor in all equity investments. The most basic risk is that future outcomes—in the form of results of operations, profitability, and share value—will not meet expectations. Risk may also be associated with volatility of revenues or any other accounting metric, changes in underlying stock value, and uncertainties regarding many variables such as exogenous economic factors; markets, market share, and competitive behavior; liquidity and the ability to produce and sustain necessary cash flows and to obtain necessary financing; management judgment; and changes in technology or customer preferences.

Investors use financial information principally to assess operating results, make judgments about probable future performance, and evaluate nonaccounting factors within the framework of a microeconomic and financial model of the enterprise in which an investment might be made. Thus, one of the greatest risks to investors is the risk that the financial information upon which they rely is materially misstated. Financial information may be misstated either erroneously or intentionally. Furthermore, financial information may be misstated by means of the inclusion of incorrect information or by excluding information. When financial information is misstated by any scheme, artifice, or device with the intent to mislead investors, it is a form of financial fraud.

Overview of Financial Information and the Requirement to Present Fairly

In U.S. capital markets, financial information reporting takes the basic form of either a general-purpose financial statement—which includes balance sheets—or a statement of financial position; a profit-and-loss statement, also known as P&L or statement of operations; a statement of changes in equity; a statement of cash flows; and footnotes that provide additional information concerning accounting policies and procedures used in preparing the financial information contained in a financial statement, the nature and composition of balances shown in a financial statement, and other significant matters requiring disclosure for a financial statement to present fairly the results of operations and the financial condition of the reporting entity. Most U.S. securities registrants are required to file certain financial information

with the SEC in various annual, quarterly, and periodic filings, including annual reports, on Form 10-K, and quarterly interim reports, on Form 10-Q. A company's annual report on Form 10-K is also required, by SEC rules and regulations, to include additional and supplemental information in the nature of certain statistical information; descriptions of the company's business, products and services, plant and properties, major operating units and their locations, and significant risk factors; management's discussion and analysis of operations, also known as MD&A; an assessment of liquidity and liquidity risks; and certain supplementary schedules such as a schedule of valuation reserves and loss accruals.

Quarterly interim information filed on Form 10-Q contains condensed financial information and abbreviated footnote disclosure to be used in conjunction with the more detailed disclosure set forth in an entity's annual report. Any other material financial disclosures—typically those that might occur during periods between annual and quarterly reporting dates—may be reported in the form of press releases such as preliminary earnings releases or, depending on their significance, in a Form 8-K filing. As a general matter, if any of these required reports contain false statements or omit significant information, they may be in violation of U.S. laws and regulations.[2]

Until recently, Generally Accepted Accounting Principles (GAAP) represented a body of authoritative guidance, promulgated by one or more of the following:

- Financial Accounting Standards Board (FASB)
- Accounting Principles Board (APB), predecessor of the FASB
- American Institute of Certified Public Accountants (AICPA), usually through its Accounting Standards Executive Committee (AcSEC)
- Emerging Issues Task Force (EITF) of the FASB

Such authoritative guidance was in the form of FASB statements of financial accounting standards (SFASs), APB opinions (APBs), AICPA statements of position (SOPs), EITF issues (EITFs), APB interpretations (AINs), FASB interpretations (FINs), FASB technical bulletins (FTBs), or FASB statements of financial accounting concepts (CONs). SEC guidance, usually in the form of staff accounting bulletins (SABs), provides insights on the SEC staff's interpretation of GAAP.

In 2009, the United States accounting and reporting standards underwent a major restructuring, and the FASB accounting standards codification became the

---

[2] Some of the most commonly cited provisions of U.S. law and regulation are Section 10(b) of the Securities Exchange Act of 1934 and corresponding Rule 10b-5, "Employment of Manipulative and Deceptive Devices," of the Securities Exchange Act of 1934 [Public Law 73-291, 73rd Cong., 2d sess., 13 (1934)]: "It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

a. To employ any device, scheme, or artifice to defraud,

b. To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or

c. To engage in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security."

single official source of authoritative, nongovernmental GAAP, superseding existing FASB, AICPA, EITF, and related literature (excluding SEC guidance). One of the primary goals in developing the codification was to simplify user access by codifying all authoritative U.S. GAAP in one spot.[3]

There has been a move toward a single set of globally accepted accounting standards over the past several years. In 2007, the SEC agreed to accept financial statements prepared in accordance with international financial reporting standards (IFRS) without reconciliation to U.S. GAAP from foreign private issuers. In 2008, the International Accounting Standards Board (IASB) and FASB reaffirmed their memorandum of understanding to converge all major accounting standards by 2011 in light of a possible move to IFRS.[4]

With this background in mind—much of it common knowledge among working auditors—we can turn to the question of what it means to present fairly the financial statements of an entity. AICPA Statement on Auditing Standard No. 69, *The Meaning of* Present Fairly *in Conformity with Generally Accepted Accounting Principles in the Independent Auditor's Report,* correlates as follows the concept of *present fairly,* in financial statements, with GAAP:

> *Judgment concerning the "fairness" of the overall presentation of the financial statements should be applied within the framework of generally accepted accounting principles. Without this framework, the auditor would have no uniform standard for judging the presentation of financial position, results of operations, and cash flows in financial statements.*

SEC Financial Reporting Practices (FRP), Section 101 (Accounting Series Release, or ASR 4, April 25, 1938) states:

> *In cases where financial statements filed with the Commission pursuant to its rules and regulations under the Securities Act or the Exchange Act are prepared in accordance with accounting principles for which there is* no substantial authoritative support, *such financial statements will be* presumed to be misleading or inaccurate *despite disclosures contained in the certificate of the accountant or the footnotes to the statements, provided the matters involved are material. [*emphasis added*]*

And SEC FRP Section 150 (ASR 150, December 20, 1973) states:

> *In the exercise of its statutory authority with respect to the form and content of filings under the Acts, the Commission has the responsibility to ensure that investors are provided with adequate information.* A significant portion of the necessary information is provided by a set of basic financial statements (including the notes thereto), which conform to generally accepted accounting principles. [emphasis added]

---

[3] FASB Accounting Standards Codification Notice to Constituents (v 3.0) *About the Codification,* 2009.
[4] "Where Will the SEC Take the IFRS Roadmap?" AICPA, April 27, 2009.

Thus, by definitions of both the AICPA and the SEC, financial statements that do not conform to GAAP are not presented fairly and are presumed to be misleading or inaccurate. When investors perceive that financial statements are misleading, a class-action lawsuit is often the result. Such lawsuits typically allege that false statements were made or material information was omitted. (See box, Elements of a Securities Class-Action Complaint.)

ELEMENTS OF A SECURITIES CLASS-ACTION COMPLAINT

1. The defendants made misleading statements and material omissions during the class period.
2. Company X securities traded on the New York Stock Exchange, which is an efficient market.
3. Company X stock price effectively reflected new information and announcements concerning the company that entered the market.
4. Company X is a regulated issuer and, as such, filed periodic public reports with the SEC.
5. Trading volume of the company's stock was substantial during the class period.
6. During the class period, Company X was followed by and regularly communicated with securities analysts employed by brokerage and research firms, who wrote reports that were distributed to the sales force and certain customers of such firms and that were available by means of various automated data retrieval services.
7. Misrepresentations and material omissions alleged in this complaint would tend to induce a reasonable investor to misjudge the value of the company's stock.
8. Plaintiff and other members of the class bought the company's securities—either at or after the time the misleading statements and material omissions were made—without knowledge of the misrepresented and omitted facts. *(This last point could alternatively be made in the context of shareholders who are selling.)*

Overview of Fraud in Financial Statements

Fraudulent financial information typically takes the form of material misstatements made either intentionally or recklessly in one or more of the foregoing types of reports. The most common vehicles are the annual and quarterly financial statements. Such misstatements generally involve overstatement of revenues; understatement of expenses; overstatement of assets; omission of liabilities; mischaracterization of, or failure to disclose, transactions, accounting events, or other information material to a fair presentation of the reported results of operations; and materially misleading disclosures in respect of MD&A; liquidity and liquidity risks; products and services and their efficacy, market success, and so on; and supplemental information.

EXHIBIT 21.1 Combinations of Misstatements in Typical Inclusive Frauds

Assets or Liabilities	Income Statement Effect
Accounts Receivable [Overstated]	Revenue [Overstated]
Allowance for Sales Returns [Understated]	Revenue [Overstated]
Doubtful Accounts Allowance [Understated]	Bad Debt Expense [Understated]
Inventory [Overstated]	Cost of Goods Sold [Understated]
Inventory Reserves (for Lower-of-Cost-or-Market Impairment) [Understated]	Cost of Goods Sold [Understated]
Inventory [Overstated]	Direct Expenses [Understated]
Prepaid or Deferred Assets [Overstated]	Direct, Indirect or Selling, General and Administrative Expenses [Understated]
Accounts Payable, or Accrued Liabilities, or Other Obligations [Understated]	Expenses [Understated]

Financial statements that are intentionally or recklessly misstated so that they are misleading or inaccurate and do not conform to GAAP, represent a fraud upon investors. The most common type of financial statement fraud involves overstatements of revenues and earnings and understatement of costs and expenses so as to inflate the profitability or minimize the losses of an entity. Concurrently, such misstatements of the P&L also result in overstatements of assets and understatements of liabilities. Such fraud also is known as an *inclusive* fraud because the financial statements *include* transactions or values that are incorrect. Alternatively, a fraud may involve the intentional omission of liabilities and obligations from the financial statements of a company. Such a fraud is known as an *exclusive* fraud because transactions that *should be included* are not. Most typically, *inclusive* frauds involve the combinations of misstatements arrayed in Exhibit 21.1.

The types of *inclusive* frauds reflected in Exhibit 21.1 may involve either the creation of fictitious assets, or the omission of actual liabilities, or both, or they may involve the timing of transactions so as to improperly reflect, for example:

- Revenues and receivables prematurely recognized before they are earned and realized or realizable
- Costs of goods sold deferred beyond when such costs should have been accrued, either by improperly overstating the value of inventories or by deferring the recognition of purchases or costs (materials, labor, and supplies) or of indirect expenses and overhead expenses
- Contingencies—in the form of doubtful accounts allowances, sales returns allowances, warranty and product liability reserves, litigation reserves, and the like—not recognized in a timely manner (when they were first *probable* and *estimable*), thus resulting in delayed recognition of associated provision expenses
- Accruals of accounts payable and other liabilities not recognized in a timely manner when the obligations actually were incurred, thereby deferring recognition of the related expenses

In the case of the creation of fictitious assets, the two most common frauds involve recording fictitious revenues and associated fictitious receivables and recording fictitious inventory and thus understating the cost of goods sold or other expense.

However, any balance sheet account for which a fictitious debit can be created can be used to create an equal and inapposite fictitious credit to post to either a revenue or an expense account in the P&L, thus overstating earnings.

Exclusive frauds typically involve the exclusion of liabilities or other obligations—such as commitments, guarantees, or contingencies—from a company's balance sheet. The effects of such exclusions can include:

- Associated understatement of an expense, such as:
  - Environmental cleanup expenses and related litigation expense provisions, associated with a failure to properly record environmental liabilities
  - Litigation expense provisions, associated with a failure to properly record litigation reserves and judgment liabilities
  - Losses associated with debts and other long-term liability obligations that inure to a company as a result of undisclosed guarantees, commitments, or other debt-related contingencies
  - Reserves or direct charge-offs associated with impairments of unconsolidated assets such as equity investments, joint ventures, and partnerships, with the failure to record such also resulting in an understatement of investment losses or impairment charges to earnings
  - Allowances or loss accruals related, among other possibilities, to doubtful account allowances, loan loss allowances, inventory reserves, warranty and product liability reserves, or self-insurance reserves that are intentionally excluded and thus result in understatement of the associated expense provisions
- Associated overstatement of liquidity measures—such as debt to equity or current ratios—and understatement of the true balance of a company's total liabilities
- Associated understatement of interest expense

Some frauds involve the intentional mischaracterization of the nature of transactions and misleading disclosures dealing with the accounting policies and procedures used to account for such transactions or events, the effects of accounting changes, the classification of transactions, or how such transactions affect reported results of operations. Among the most common examples are:

- Failure to properly disclose the effects—on both current and, possibly, future operations—of material changes in accounting estimates.
- Misclassification of operating expenses and costs or losses as nonrecurring, when in fact such expenses should be reflected as operating.
- Creation of reserves—most typically associated with pre-acquisition liabilities, restructuring charges, and other so-called one-time charges—intentionally exceeding probable and estimable liabilities expected to be incurred as well as the subsequent release of such reserves so as to offset expenses or increase revenues for which such reserves were not provided. In many cases, the provisions of such reserves are reflected as nonoperating charges, while their subsequent release, in whole or in part, is reflected improperly as results of continuing operations incurred in the ordinary course of business.
- Misstatement of—or failure to include—key accounting policies or their effect upon reported results of operations or both.

Another type of financial fraud involves the intentional creation of *cookie jar reserves*—that is, general reserves of the kind that are prohibited under ASC 450 *Contingencies*. This usually occurs in times when a company is enjoying excess earnings—meaning, earnings that exceed the company's profit plan and analysts' consensus on earnings expectations. The excess is kept for a rainy day, when release of such reserves helps the company achieve earnings targets, absent which the company's results of operations would not meet market expectations. Just about any allowance, loss accrual, or reserve account will do as a cookie jar. The only common denominator is the intentional provision or maintenance of reserves or both in excess of contingent liabilities that are specifically identifiable and are both *probable* and *estimable* under the criteria set forth in ASC 450 *Contingencies*.

Accounting Irregularities as an Element of Financial Fraud

SAS No. 99, *Consideration of Fraud in a Financial Statement Audit,* defines financial fraud that involves accounting irregularities, as follows:

> *Misstatements arising from fraudulent financial reporting are intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. Fraudulent financial reporting may involve acts such as the following:*
>
> *Manipulation, falsification, or alteration of accounting records or supporting documents from which financial statements are prepared*
>
> *Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information*
>
> *Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure*[5]

Generally, badges of financial fraud include:

- Reported results that do not comport with GAAP (although GAAP violations alone do not necessarily mean fraud).
- Pressures or incentives to commit fraud, including pressure to achieve unrealistic operating results and incentives in the form of performance-based compensation such as stock options, bonuses, or other forms of performance-based compensation, the value of which is tied to achieving such unrealistic operating results.
- Opportunities to commit fraud, resulting from lack of adequate controls, insufficient segregation of duties, or dominance by one or more individuals over critical elements of the accounting and reporting process.
- Concealment through falsification, alteration, destruction, or the hiding of documents and other accounting evidence.

[5] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par 6.

- Collusion, attributable to the belief that just one person alone rarely perpetrates major financial frauds: Instead, major financial frauds typically involve and require acts, by commission or omission, by a number of individuals.
- Misrepresentations about a wide variety of factors: saying control activities have been performed properly, when in fact they have not; the true nature of transactions or accounting events; management's true intent in respect of transactions being entered into; the reasonableness and support for management's judgments and estimates, when such are in fact known to be unreasonable or lacking in valid support; or false evidence, misrepresented to be true and valid, again regarding a wide variety of possible factors: absence of side letters; authenticity of documents known to have been falsified or otherwise altered; relationships with counterparties, including concealment of related party arrangements; the dating of documents—such as backdating—and actual timing of transactions; and the true nature of arrangements such as those concerning rights of return, contingent arrangements, consignment arrangements represented to be completed sales, and undisclosed rebates and other price concessions.

Ponzi Schemes In 1919 and 1920, Charles Ponzi operated an investment scheme through his business, Securities Exchange Co., which promised investors returns of up to 50 percent, purportedly to be earned from investing in and arbitraging International Postal Union reply coupons. In reality, after some initial success in his venture, Ponzi sustained losses and to keep the scheme going, began repaying old investors with funds provided by new investors. Although Ponzi was exposed, jailed, and eventually exiled back to Italy, where he died penniless, his name lives on to identify a kind of financial fraud that depends on claims of astonishing profits to investors in the form of rates of return, on attracting more and more new investors to provide the funds with which to repay old investors, and on a pyramid structure in which only the initial investors and the sponsor of the scheme recover their investments and earn profits thereon. Modern versions of Ponzi schemes may involve multiple pledging of assets claimed to be security for the investors' loans or other investments, commingling of funds and diversion of cash collateral, and fraud in the inducement to invest by:

- Mischaracterizing the nature of, and risks associated with, the investment
- Overstating anticipated returns and misstating the security backing up the investment
- Misstating financial statements by overstating investment returns and operating results or understating losses or both
- Misrepresenting the success of the product, service, or financial scheme upon which the investment is to be based
- Concealing losses and the failure of the scheme—at least for a time—by paying out later investors' monies to earlier investors

During the last decade Ponzi schemes have remained popular. The SEC reports that it has filed 55 cases involving Ponzi schemes or Ponzi-like payments in 2009

alone.[6] Several recent cases over the last several years have been of significant size and public interest, for example, the investment fund scheme managed by Bernard Madoff and the bank deposit scheme at Sanford Bank in Texas. These schemes illustrate the continuing power of the promise of better-than-average investment returns in the hands of a skilled fraudster.

Bank Frauds Although they are not usually investors in equity securities, banks invest in loans to entities that are based at least in part on reliance upon the financial statements and other financial information provided by the borrower. Thus, fraudulent financial statements may be used to defraud lenders just as they defraud equity investors, usually by overstating a company's financial condition and results of operations. Several additional forms of fraud may also affect lenders. They typically involve overstating the value of collateral, pledging fictitious collateral, multiple pledging of assets as security, and fraudulently conveying assets—against which loans were made—to related parties, third parties, or other lending institutions. In the recent mortgage crisis the inflation of home values by appraisal companies was so widespread, the U.S. government is taking action to criminalize such activity. The requirements in the Fraud Enforcement and Recovery Act of 2009 (FERA) make it a crime to overstate the value of the property collateralizing a mortgage. FERA also improves enforcement of securities fraud and commodities fraud, financial institution fraud, and other frauds related to federal assistance and relief programs for the recovery of funds lost to these frauds, and for other purposes.[7]

Fraud on Auditors The purpose of an independent audit is to determine whether financial statements do in fact present fairly the financial condition and results of operations of a company in accordance with GAAP. If reported results contain accounting irregularities and do not comply with GAAP, any intentional failure to disclose such a condition represents a fraud perpetrated on the auditors. This type of fraud has as its purposes obtaining from the auditors an unqualified audit opinion and keeping the auditors from knowing about and disclosing the accounting irregularities. Fraud on auditors typically includes some combination of the following elements:

- Misrepresentations by management or employees or both concerning the nature of transactions, the accounting applied, the absence of accounting irregularities—when in fact such accounting irregularities exist—and adequacy of disclosure
- Concealment of fraudulent transactions by means of falsification, alteration, and manipulation of documents and accounting records or, in some cases, by keeping a separate set of books and records

[6] Robert Khuzami, director, Division of Enforcement, U.S. Securities and Exchange Commission, "Testimony Concerning Mortgage Fraud, Securities Fraud, and the Financial Meltdown: Prosecuting Those Responsible," December 9, 2009.
[7] Fraud Enforcement and Recovery Act of 2009, www.gpo.gov/fdsys/pkg/PLAW-111publ21/content-detail.html.

- Subornation of collusion to defraud from among management or employees or both, taking the form of silence when in fact these persons have knowledge of the fraudulent activities but do not disclose their knowledge to the auditors, active participation in the fraud by corroborating misrepresentations or assisting in the falsification of books and records or both, and assistance in the circumvention of internal controls designed to prevent or detect fraud
- Collusion with third parties or other employees of the victim company, in which such parties are aware of irregular transactions but do nothing to prevent them or nothing to bring them to the attention of either their auditors or the counterparty's auditors
- Deceptions, including planning the fraud to take advantage of known or anticipated patterns of auditing—such as scope of testing or audit locations—and furnishing false information to auditors in response to their audit inquiries
- Destruction of evidential matter or withholding key documents or both, such as side letters

Lying to an auditor can also result in criminal sanctions. According to the U.S. Department of Justice, lying to auditors or a forensic accounting investigator can be considered obstruction of justice. Also, lying to any member of an audit team may trigger penalties under Sarbanes-Oxley (misleading an auditor).

SOME OBSERVATIONS ON FINANCIAL FRAUD

According to the 2009 Securities Litigation Study,[8] the number of federal securities class actions from the plaintiffs' bar dropped to 155 cases compared to 210 cases in 2008. Specific accounting-related allegations in 2009 included estimate-related allegations, internal controls, overstatement of assets, revenue recognition and understatement of liabilities and expenses and 47 and 33 percent of the 2008 and 2009 filings related to the financial crisis, respectively. Even with such a small number of cases relative to total SEC registrants, the incidence of allegations of financial fraud is shocking to U.S. capital markets and to investors.

Financial fraud may be minimized and reduced in its effects on capital markets and investors if it is sought out and recognized in its early stages. Most financial frauds start small and then grow bigger and bigger until they cause significant harm. The application of sufficient vigilance and professional skepticism may serve as deterrents to financial fraud and the attendant financial losses suffered by investors and other users of financial information. Experience has shown that adequate internal controls, proper tone at the top, effective auditing, and alertness to fraudulent activities can make a real difference.

Fraud from Within

At the beginning of this chapter, we said certain capital market participants—generally, financial institutions such as banks, insurance companies, broker-dealers,

[8] PricewaterhouseCoopers, 2009 Securities Litigation Study.

and investment banks—are sometimes defrauded by their own employees. Some of these instances are relatively straightforward thefts of an employer's assets or of customer assets in the custody of the institution. For example, a loan officer might create false borrowing requests to draw on borrowing facilities and then circumvent confirmation and statement delivery procedures to keep the customer from learning of the misappropriation. Alternatively, more complex trading schemes are sometimes developed—normally, from a desire to hide losses incurred in trading activities that exceeded the limits of the employee's authority. This type of fraud can be extremely harmful to the institution because huge debts can quickly mount beyond the financial capacity of the institution to repay.

SUMMARY

In the current financial accounting and reporting environment, the temptations to commit accounting irregularities can be great. The value of performance-based compensation—especially the value of options, bonuses, and other variable compensation awards for CEOs, CFOs, and other senior management—often acts as a strong lure to manage earnings, set unrealistic revenue and profit targets, and manipulate accounting to achieve results in line with market expectations. The pressures of competition, technology change, and the need for capital sometimes cause some people to do dumb things, including perpetration of financial fraud. Furthermore, because of the waves of lucrative IPOs in the 1990s and the significant growth of middle-market firms, the accounting bench of properly trained, suitably experienced, and ethically aware financial officers became lean. The traditionally rigorous system of training, developing, supervising, and promoting accountants gave way in some companies to instant accountancy among inexperienced accountants, younger MBAs, and others who lacked the appropriate knowledge, experience, and professional discipline to properly perceive the difference between what is right and what is wrong in accounting judgments. Some of these people were swayed by senior management to act in ways that put company performance before ethical values.

The SEC and the Justice Department, as well as many state regulatory agencies and judicial departments, have increased their focus on, and activities involving, financial fraud. The penalties, both civil and criminal, for financial fraud are severe, and recent investigations and prosecutions of alleged financial frauds have been tenacious and thorough. Likewise, the auditing profession has experienced a wake-up call regarding financial fraud and has become even more sensitive to, and vigilant for, any instances that suggest irregularities or improper accounting. Although it will always be true that some people think the rules apply only to others and not to themselves, the message is clear: Many financial frauds are caught and the perpetrators punished. Increased vigilance will push those statistics even higher.

However, even one financial fraud that is spectacular in terms of size, audacity, and harm can do enormous damage to investor confidence in financial markets, the strength of financial institutions, and the reliability of financial statements. Even though the incidence of financial statement fraud is low relative to the total number

of companies with shares traded on U.S. and foreign exchanges, the economic losses associated with a small number of recent financial frauds have been enormous and shocking to investors, financial analysts, accounting professionals, and regulators. More needs to be done to deter, detect, and expose such financial frauds to better sustain confidence in the system of financial reporting and audit assurance that underpins U.S. capital markets.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 22

Financial Statement Fraud: Revenue and Receivables

Jonny J. Frank, David Jansen, and Michael Carey

Overstating revenue is one of the most common of all financial statement fraud schemes. As a result, the Statement on Auditing Standards (SAS) 99, *Consideration of Fraud in a Financial Statement Audit*, includes a presumption that improper revenue recognition is a fraud risk.[1] According to the 2010 report by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the most common fraud technique involved improper revenue recognition, followed by the overstatement of existing assets or capitalization of expenses. Revenue frauds accounted for more than 60 percent of the 347 alleged cases of public company fraudulent financial reporting from 1998 to 2007.[2] More broadly speaking, many fraudulent financial reporting schemes involve earnings management, which the U.S. Securities and Exchange Commission (SEC) has defined as "the use of various forms of gimmickry to distort a company's true financial performance in order to achieve a desired result."[3]

Earnings management does not always involve outright violations of Generally Accepted Accounting Principles (GAAP). Companies may try to manage earnings by choosing accounting policies to attain earnings targets. There is a difference between such technique and those that clearly violate GAAP. At the same time, it should be noted that the SEC has cautioned that compliance with GAAP is not a protection against an enforcement action if financial performance is distorted.[4]

---

[1] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par. 41.
[2] Committee of Sponsoring Organizations of the Treadway Commission, *Fraudulent Financial Reporting: 1998–2007, an Analysis of U.S. Public Companies* (New York: COSO, 2010), Executive Summary, III.
[3] U.S. Securities and Exchange Commission, *Annual Report* (SEC, 1999), 84.
[4] The SEC's enforcement action against Edison Schools (Edison) is illustrative; Securities Exchange Act of 1934 (SEA) Rel. No. 45925, Accounting and Auditing Enforcement (AAE) Rel. No. 1555 (May 14, 2002). Edison operates public schools on behalf of local governments, which paid directly certain school expenses. Edison Schools recognized these payments as

There are many aspects of GAAP that require management to make a judgment, which makes the application of GAAP more an art than a science. As a simple example, GAAP allows any depreciation method so long as it systematically and rationally allocates the cost of an asset over its useful life. GAAP also allows various methods of inventory valuation, including last in, first out; first in, first out; and specific identification.[5] Other instances in which management must make judgments include:

- Changing depreciation methods from an accelerated method to the more conservative, straight-line method or vice versa
- Changing the useful lives or estimates of the salvage value of assets
- Determining the appropriate allowance required for uncollectible accounts receivable
- Determining whether and when assets have become impaired and are required to be reserved against or written off
- Determining whether a decline in the market value of an investment is temporary or permanent
- Estimating the write-downs required for investments

The SEC has noted that accounting principles are not meant to be straitjackets, and a degree of accounting flexibility is essential to innovation.[6] As former SEC chairman Arthur Levitt noted in 1998, accounting and reporting abuses occur only when this flexibility is exploited to distort the true picture of the corporation.[7]

Companies have a host of reasons for exercising their judgment in applying those principles that will paint the healthiest financial picture, but typically, the most powerful reason is that the market is looking for positive results. That expectation is reflected in the stock price punishment often endured by companies if their reported earnings fall short of estimates, sometimes even by a penny. Yet market pressure to meet earnings estimates is in direct conflict with market pressure for transparency in financial reporting.

It can be a difficult challenge for auditors to distinguish between aggressive but allowable accounting and accounting that is abusive and prohibited. The key determinant is management's intent. Fraud rarely occurs if management's intent is transparent and clearly understandable, but what if management selects a policy it knows will have both a positive and a negative effect on the financial picture—and refuses to recognize the negative effect? Does that demonstrate fraud in the selection of the policy? A difficult question, to be sure. Auditors who encounter such a situation in actual practice may counsel with others and gather facts before drawing any conclusions.

---

revenue, even though the payments did not flow through its accounts. The SEC launched an enforcement action notwithstanding that the accounting technically complied with GAAP.

[5] See ASC 360–10-35 "Assets, Property, Plant, and Equipment, Overall, Subsequent Measurement, Depreciation."

[6] Arthur Levitt, "The 'Numbers Game,' " Speech, New York University Center for Law and Business, September 28, 1998, www.sec.gov/news/speech/speecharchive/1998/spch220.txt.

[7] Id.

Beyond areas of legitimate managerial judgments lie frauds that are clearly outside the parameters of GAAP. These techniques may inflate earnings, create an improved financial picture, mask a deteriorating trend, or hold back earnings for later release.

Financial statement fraud is based on deceptively altering the accounting records of a company so as to improperly reflect one or more of the records' basic elements: assets, liabilities and equity, revenues, and expenses. In many schemes, the requirements of double-entry bookkeeping result in two or more of these basic categories being misstated. Some frauds, such as recognition of inventory but not the payable for it, are based on one-sided accounting entries, often accomplished through a subsidiary ledger or record that is incompletely reconciled to the general ledger. The fraud schemes that are the focuses of this chapter—revenue and receivable schemes—are generally accomplished by increasing both revenue and receivable accounts.

IMPROPER REVENUE RECOGNITION

A number of reports and studies have found that from 1981 to 2008, approximately one-half or more of SEC enforcement actions and shareholder actions involved improper revenue recognition. Improper recognition can take two forms: either premature recognition of revenue generated through legitimate means or recognition of fictitious revenue from false sales or to false customers. Overstated revenue can come about by means of:

- Accelerating shipments or holding the books open for sales made subsequent to the end of the accounting period
- Recognizing revenue for transactions that do not actually qualify as sales, such as consignment sales not yet sold to the end user, sales with special conditions, certain bill-and-hold transactions, products shipped for trial or evaluation purposes
- Executing sham sales transacted for the purpose of increasing sales volume, such as swaps or round-trip trades and related party transactions
- Overstating percentage-of-completion sales
- Failing to reduce gross sales for all appropriate adjustments from gross to net—that is, understatement of returns, allowances, or discounts, including prompt payment discounts and product markdowns
- Recording fictitious sales

Inquiries into suspected improper revenue recognition usually begin with a review of revenue recognition policies and customer contracts. The auditor may consider the reasonableness of the company's normal practices in the context of accepted revenue recognition practices in the relevant industry and whether the company has complied with them. For example, if a company customarily obtains a written sale agreement, the absence of a written agreement may be a red flag. The review may begin with a detailed reading of the contract terms and provisions. Particular attention may be focused on terms governing payment and shipment, delivery and acceptance, risk of loss, terms requiring future performance on the part of the seller

before payment, payment of upfront fees, and other contingencies. A review for these issues as well as others is designed to focus on the general requirements for revenue recognition set forth in GAAP.

- The SEC has interpreted GAAP requirements in Staff Accounting Bulletin (SAB) 101, *Revenue Recognition in Financial Statements*,[8] as amended by SAB 104, which spells out four basic criteria that must be met before a public company may recognize revenue:
  - Persuasive evidence that an arrangement exists
  - Evidence that delivery has occurred or that services have been rendered
  - A showing that the seller's price to the buyer is fixed or determinable
  - Reasonable assurance of the ability to collect payment

SAB 104 echoes the recognition requirements originally listed in the American Institute of Certified Public Accountants (AICPA) Statement of Position 97–2, *Software Revenue Recognition*,[9] which governs the software industry. SAB 104 states that whenever industry-specific authority exists, companies may comply with that authority rather than follow SAB 104.

Timing

The auditor may also consider timing, particularly as it relates to the company's quarterly and year-end periods. In which periods were the sales agreements obtained? When was the product or equipment delivered? When did the buyer become obligated to pay? What additional services were required of the seller? As these questions suggest, the timing of transactions can be manipulated to accelerate revenue

[8] U.S. Securities and Exchange Commission, Staff Accounting Bulletin (SAB) 101, *Revenue Recognition in Financial Statements,* 17 CFR Part 211 (December 3, 1999), was updated by SAB 104: *Revenue Recognition, Corrected Copy,* 17 CFR Part 211 (December 17, 2003). SAB 104 revises or rescinds portions of the interpretative guidance included in Topic 13 of the codification of staff accounting bulletins so it can make this interpretive guidance consistent with current authoritative accounting and auditing guidance and SEC rules and regulations. The principal revisions relate to the rescission of material no longer necessary because of private-sector developments in U.S. Generally Accepted Accounting Principles. It also rescinds the document *Revenue Recognition in Financial Statements: Frequently Asked Questions and Answers,* issued in conjunction with Topic 13. Selected portions of that document have been incorporated into Topic 13. While we recognize that many in the accounting profession refer to SAB 101 as the source of SEC guidance on revenue recognition, throughout this book we will refer to SAB 104 because it incorporates and amends SAB 101 for recent developments in the profession. The codified texts of SABs 101 and 104 are available on the SEC web site at www.sec.gov/interps/account/sabcodet13.htm, SEC Staff Accounting Bulletin: Codification of Staff Accounting Bulletins, Topic 13: Revenue Recognition, subsection: Persuasive evidence that an arrangement exists.

[9] American Institute of Certified Public Accountants, Statement of Position (SOP) 97–2, October 27, 1997; SOP 98–9, Modification of SOP 97–2, "Software Revenue Recognition With Respect to Certain Transactions."

recognition. When the timing of recognition is manipulated, the offending company may be facing:

- Pressure to meet revenue targets as the accounting period—that is, the quarter—comes to a close.
- A known or expected shortfall of sales transactions actually consummated through period end.
- The potential existence of sales that are expected to be consummated shortly after period end.
- Opportunity either unilaterally or in collusion with customers—that is, counterparties—to alter the dating of these post-period-end transactions so as to make such transactions appear to have been consummated before the period-end close of business.

Red flags in this area may include:

- Falsification or alteration of documents, including backdating of delivery or shipping documents
- Backdating or alteration of the dates of invoices
- Alteration or falsification of other dating evidence that might reveal the true date(s)—post-period-end—of the arrangement or of delivery of the products sold or services rendered

Some examples of other dating evidence that may require alteration include:

- Facsimile dates such as on copies of signed contracts or other documents.
- Management information system transaction record dating.
- Sales registers or sales journals transaction dates.
- Purchase order dates: It could be incongruent and difficult to explain that the date of a purchase order was later—that is, after period end—than the purported dates falsely entered on contracts, invoices, and delivery documents.
- Dating of correspondence associated with negotiation and consummation of the transaction.

A necessary result of any timing irregularity in accounting is that the current accounting period borrows revenues from the next period or periods, thus starting these subsequent periods off in the hole. If the next periods also have flat or declining actual sales—thereby exacerbating the revenue shortfall already created by the timing irregularity—even more premature revenue recognition accounting irregularities will be needed at the affected period ends to:

- Make up the shortfall caused by lending revenues to the previous period
- Cover the effects of any real decline in sales
- Achieve the expected level of sales growth

At a time when real sales are declining and such timing irregularity accounting is taking place, each period may require more and more fraudulent premature revenue

recognition in order to keep up the appearance—and the fiction—that revenues are growing.

The recognition of revenue transactions may occasionally go in the opposite direction and can be improperly delayed—when, for example, sales expectations (either internal or external) have already been met and the company wishes to defer recognition of revenue into the following accounting period. (See also "Cookie Jar Reserves" in Chapter 23.)

REVENUE RECOGNITION DETECTION TECHNIQUES

Auditors have a variety of detection tools and techniques to use in the revenue recognition area, ranging from inquiry of relevant managers and substantive analytical tests of account balances to calling in forensic accounting investigators to investigate suspected improprieties. General detection techniques specific to revenue recognition may include the following:

- Discuss with both sales and marketing and financial personnel whether, how, and during which time period revenue targets were achieved; discuss, as well, sales that occurred near the end of the accounting period.
- Perform cutoff testing to determine whether sales were accelerated or decelerated:
  - Examine purchase orders, invoices, and shipping documents.
  - Compare shipping volumes with volumes billed.
  - Examine ending inventory.
  - Look for document predating or postdating.
  - Make inquiries of employees in the shipping area. Topics may include large shipments near period end, large returns, bill-and-hold transactions, and the like.
- Analyze large sales transactions, especially those occurring:
  - Near the end of the accounting period
  - With a new customer
  - With a related party
- Physically observe goods being shipped.
- Analyze new customers making large purchases:
  - Confirm physical location (rather than a post office box).
  - Consider comparing entity address with employee addresses.
  - Consider confirming existence through public records search.
  - Review post-closing transactions for evidence of invoicing and payment of invoice or, alternatively, cancellations or returns.
- Look for unrecorded and unprocessed returns, whether physically returned or shipped to an offsite warehouse, and those the company has made a commitment to accept.
- Inquire about side agreements—such as return rights, cancellation provisions, and other guarantees—and inquire of those outside the financial or accounting function as well as of large customers or customers placing purchases late in the reporting period.

- Analyze sales returns or contract cancellations recorded subsequent to the end of the period.
- Send confirmations to customers covering quantities, dollar amounts, dates, and side agreements.
  - Consider oral confirmations in addition to written confirmations.
  - Follow up on unreturned confirmations or confirmations returned with discrepancies.
- Review non-system-generated—that is, manual—sales journal entries.
- Independently verify estimates for percentage of completion.
- Identify customers or employees and other related parties that are also vendors, and analyze transactions with those entities.
- Perform analytical procedures on relationships with sales, including disaggregated sales data. (See discussion later in this chapter.)

The auditor may consider substantive testing as a starting point and comb through materials to see if evidence supports the existence of a fraudulent scheme—for example, by requesting and reviewing contracts and support for invoices and deliveries and going on to confirm with customers the existence of accounts receivable and the amount of consigned goods. The auditor may also consider examining public records, when available, and performing background checks on or making site visits to customers, vendors, and other third parties to verify their existence.

In examining specific accounts, the auditor may consider supporting documentation, focusing in particular on round-dollar entries at the end of periods. An auditor who finds entries that are accruals may seek supporting evidence for material reversals and confirm the proper timing of the entries.

Absent a written agreement, auditors may consider other evidence of transactions, such as purchase orders, shipping documents, and payment records. They may also consider SAB 104 as well as the accounting literature for specific industries. Companies engaged in business over the Internet, for example, face unique revenue recognition issues. ASC 605–45–05 Overview and Background, "Revenue, Revenue Recognition, Principal Arrangement Considerations," [10] attempts to solve this problem by listing factors the SEC considers in determining whether revenue should be reported on a gross or net basis. Similarly, ASC 605–50–05 "Revenue, Revenue Recognition, Principal Arrangement Considerations, Disclosure,"[11] addresses such sales incentives as discounts, coupons, rebates, and free products or services offered by manufacturers to customers of retailers or other distributors. Being aware of the applicable authority may assist the auditor in recognizing violations.

When suspicions of improper revenue recognition exist, auditors may turn to forensic accounting techniques to dig more deeply. Those techniques may range from analytical procedures to analyzing round-dollar period-end journal entries by means of data mining. A forensic accounting investigator can assist the financial auditor in determining next steps to perform and the advisable sequence of steps.

---

[10] ASC 605–45–05 Overview and Background, "Revenue, Revenue Recognition, Principal Arrangement Considerations."
[11] Id.

ANALYTICAL PROCEDURES TO IDENTIFY OR EXPLORE POTENTIAL REVENUE RED FLAGS

Analytical procedures, especially those performed on a disaggregated basis, often are useful audit tools in identifying potential revenue recognition red flags, and they can help the auditor assess fraud risk factors related to revenue recognition. However, analytics and tests are not substitutes for a good understanding of the client's business. Even seasoned auditors have been misled into believing revenue to be appropriate because they did not fully understand the business. A good question for auditors to ask themselves is, "Does this information and the results obtained make sense in light of the client's industry and business?" Comparing the client's performance against competitors' is a good way to start answering that question along the following dimensions, depending upon the circumstance:

- Reviewing balances in revenue-related accounts for unusual changes
- Calculating the percentage of sales and receivables to the total balance sheet in the current period, comparing it with prior periods, and inquiring about any unusual changes
- Reviewing cash flows to determine if cash collected is in proportion to reported revenues
- Reviewing sales activity for the period and noting unusual trends or increases, particularly near the end of the period

Significant, unusual, or unexplained changes in certain ratios may also signify areas for further pursuit:

- Increases in net profit margin (net income/total sales)
- Increases in gross profit margin (gross profit/net sales)
- Increases in the current ratio (current assets/current liabilities)
- Increases in the quick ratio (cash and receivables and marketable securities/current liabilities)
- Increases in the accounts receivable turnover (net sales/accounts receivable)
- Increases to day sales outstanding (accounts receivable turnover/365)
- Increases in sales return percentages (sales returns/total sales)
- Increase in asset turnover (total sales/average total assets)
- Increases in working capital turnover (sales/average working capital)
- Decreases in accounts receivable allowance as a percentage of accounts receivable (allowance/total accounts receivable)
- Decreases in the bad debt expense or allowance accounts

While the preceding procedures focus primarily on the income statement and the sales side of the revenue recognition issue, the balance sheet side of the equation is an additional consideration. Overstatement of accounts receivable balances can be due to improper valuation and the booking of fictitious or accelerated sales. Only the anticipated collectible value of accounts receivable should be reflected on the balance sheet, and receivables should be written down for uncollectible accounts. Also,

inflating accounts receivable with fictitious entries is a common scheme to overstate an entity's financial condition. Most frequently, when the fictitious receivables are booked, the corresponding credit is to sales. Falsified sales invoices are normally created to support the fictitious sale and receivable, often by creating phantom customers or hiding fake transactions in the records of large legitimate customers with voluminous activity. Because receivables have to be collected, written off, or disguised in some manner, such as re-aging, they are often the small but visible loose thread that unravels a revenue recognition fraud.

Detection techniques specific to receivables include the following:

- Making oral inquiries of customers regarding receivable balances.
- Researching discrepancies between the company's records and confirmation replies.
- Reviewing subsequent collections.
- Examining credit agency or analyst reports on key customers.
- Researching discrepancies between the subsidiary accounts receivable ledger and the general ledger.
- Testing the aging of accounts receivable and, in particular, considering whether accounts can be re-aged.
- Examining manual or nonsystem journal entries affecting the receivables or sales accounts: Journal entries of this type are a relatively uncommon means of recording sales.
- Investigating consistent or excessive patterns of partial payments, which may indicate kiting.
- In the case of fictitious accounts receivable, techniques related to identifying fictitious sales would be applicable.
- Performing analytical procedures on receivables (see Chapter 13).
- Testing receivables and inventory as a percentage of current assets—the higher the percentage, the higher the risk—and performing other analytical procedures on inventory, including the examination of data on a disaggregated basis (discussed later in this chapter).

Side Agreements

SAB 104 requires a definitive sales or service agreement. However, customer–vendor relationships are often complex and ever changing, and this can make it difficult for businesses to reach definitive agreements. Problems may arise when a company enters into an arrangement but later makes changes by means of a further written or oral agreement, sometimes executed outside normal control and reporting channels. Modifications made to basic or original agreements as a way of boosting sales figures have become pejoratively known as "side letters" or "side agreements." Side agreements created outside normal channels can be used to perpetrate a number of the schemes discussed in this chapter.

Depending on the business, the existence of numerous side agreements may be a red flag and might lead the auditor to conduct a detailed inquiry covering how, when, and why the agreements were entered into. If side agreements exist,

determine whether they were prepared outside normal reporting channels. If so, that could be a potential red flag. Among the fraud schemes associated with side agreements are granting customers certain liberal or unconditional rights of return, allowing customers to cancel orders at any time, extending payment terms, and misappropriation schemes perpetrated by sales staff to inflate their commissions.

The case of U.S. Foodservice, Inc., a subsidiary of Royal Ahold, illustrates the improper use of side agreements. The SEC alleged that several individuals at the company engaged in a massive financial fraud involving materially false audit confirmations. The SEC complaint alleged that U.S. Foodservice personnel contacted vendors and urged them to sign and return the false confirmation letters. In some cases, U.S. Foodservice pressured the vendors; in other cases, they provided side letters to the vendors assuring the vendors that they did not owe U.S. Foodservice the amounts reflected as outstanding in the confirmation letters. The letters clearly stated that the confirmations were being used in connection with the annual audit and the letters directed the defendants to return the confirmations directly to the company's auditors. The amounts overstated in the confirmations were often inflated by millions of dollars and by more than 100 percent.[12]

The detection of side agreements is a potentially difficult audit issue because the files and knowledge of them may not be resident in the centralized accounting departments that auditors most frequently deal with. Inquiry across a fairly broad range of company personnel may be the most important audit step. Auditors may inquire of management, accounting, salespeople, sales support staff, customer service representatives, and distribution managers as to the existence and treatment of side agreements that modify sales in any way. The auditor may also ask salespeople whether they are allowed or encouraged to use side letters or agreements to complete a sale and whether these agreements are made transparently in keeping with established reporting channels.

In addition to inquiring directly, auditors may review the company's return policies and seek to understand their rationale. They may also choose to review a sample of contracts for side agreements and confirm with a sample of customers the terms of their contracts, including the existence or absence of side agreements.

Liberal Return, Refund, or Exchange Rights

Most industries allow customers to return products for any number of reasons. *Rights of return* refers to circumstances, whether as a matter of contract or of existing practice, under which a product may be returned after its sale either in exchange for a cash refund, or for a credit applied to amounts owed or to be owed for other products, or in exchange for other products. GAAP allows companies to recognize revenue in certain cases, even though the customer may have a right of return. ASC 605–15–05–3,4,5 "Revenue, Revenue Recognition, Products, Overview and Background, Right of Return,"[13] provides that when customers are given a right of return, revenue may be recognized at the time of sale if the sales price

[12] SEC Rel. No. 19454; AAE Rel. No. 2341 (November 2, 2005).
[13] ASC 605–15–05–3,4,5 "Revenue, Revenue Recognition, Products, Overview and Background, Right of Return."

is substantially fixed or determinable at the date of sale, the buyer has paid or is obligated to pay the seller, the obligation to pay is not contingent on resale of the product, the buyer's obligation to the seller does not change in the event of theft or physical destruction or damage of the product, the buyer acquiring the product for resale is economically separate from the seller, the seller does not have significant obligations for future performance or to bring about resale of the product by the buyer, and the amount of future returns can be reasonably estimated.[14]

Sales revenue not recognizable at the time of sale is recognized either once the return privilege has substantially expired or if the aforementioned conditions have been subsequently met. Companies sometimes fail the requirements of SFAS 48 by establishing accounting policies or sales agreements that grant customers vague or liberal rights of returns, refunds, or exchanges; that fail to fix the sales price; or that make payment contingent upon resale of the product, receipt of funding from a lender, or some other future event.

Payment terms that extend over a substantial portion of the period in which the customer is expected to use or market the purchased products may also create problems. These terms may effectively create consignment arrangements, because no economic risk has been transferred to the purchaser. As noted at greater length later in this chapter, consignment sales cannot be recorded as revenue.

Frauds in connection with rights of return typically involve concealment of the existence of the right—either by contract or arising from accepted practice—or departure from the conditions of SFAS 48. Concealment usually takes one or more of the following forms:

- Use of side letters—created and maintained separate and apart from the sales contract—that provide the buyer with a right of return
- Obligations by oral promise or some other form of understanding between seller and buyer that is honored as a customary practice but arranged covertly and hidden
- Misrepresentations designed to mischaracterize the nature of arrangements, particularly in respect of:
  - Consignment arrangements made to appear to be final sales
  - Concealment of contingencies—under which the buyer can return the products—including failure to resell the products, trial periods, and product performance conditions
  - Failure to disclose the existence—or extent—of stock rotation rights, price protection concessions, or annual returned-goods limitations
  - Arrangement of transactions—with straw counterparties, agents, related parties, or other special-purpose entities—in which the true nature of the arrangements is concealed or obscured, but, ultimately, the counterparty does not actually have any significant economic risk in the sale

Sometimes the purchaser is complicit in the act of concealment—for example, by negotiating a side letter—and this makes detection of the fraud even more difficult.

---

[14] ASC 605–15-15–1,2,3,4 "Revenue, Revenue Recognition, Products, Overview and Background, Scope and Scope Exceptions."

Furthermore, such frauds often involve collusion among a number of individuals within an organization, such as salespersons, their supervisors, and possibly both marketing and financial managers.

In 2004, the SEC charged two former executives of Clarent Corporation for allegedly inflating Clarent's revenues through fraudulent sales transactions. According to the SEC, the defendants carried out the improper revenue recognition scheme by immediately recognizing revenue from transactions in which customers had been given the right to return products, the right to cancel orders, or a guarantee that Clarent would find a purchaser for any product customers were unable to sell on their own. The alleged purpose of the scheme to defraud was to falsely inflate Clarent's revenue and profits, to meet or exceed projected quarterly financial results, to induce investors to continue to purchase and hold Clarent's stock, to artificially sustain Clarent's stock price, to permit the defendants to enrich themselves, and to maintain the defendants' positions in the company and reputation with the investing public and companies with which Clarent did business.[15]

As with side agreements, a broad base of inquiry into company practices may be one of the best assessment techniques the auditor has regarding returns and exchanges. In addition to inquiries of this kind, auditors may use these analytics:

- Compare returns in the current period with prior periods and ask about unusual increases.
- Because companies may slow the return process to avoid reducing sales in the current period, determine whether returns are processed in a timely fashion. (This may require a visit with warehouse personnel.) The facts can also be double-checked with customers.
- Calculate the sales return percentage (sales returns divided by total sales) and ask about any unusual increase.
- Compare returns subsequent to a reporting period with both the return reserve and the monthly returns to determine if they appear reasonable.
- Determine whether sales commissions are paid at the time of sale or at the time of collection. Sales commissions paid at the time of sale provide incentives to inflate sales artificially to meet internal and external market pressures.
- Determine whether product returns are adjusted from sales commissions. Sales returns processed through the so-called house account may provide a hidden mechanism to inflate sales to phony customers, collect undue commissions, and return the product to the vendor without being penalized by having commissions adjusted for the returned goods.

Channel Stuffing

Channel stuffing is the practice of offering deep discounts, extended payment terms, or other concessions to customers to induce the sale of products in the current period when they would not otherwise have been sold until later. The scheme has been widely used by companies that sell goods through mass-market outlets, such as department stores, home centers, or grocery stores. In some industries, the practice

[15] SEC Rel. No. 18915; AAE Rel. No. 2118 (September 30, 2004).

is known as *loading* and occurs at the end of virtually every quarter. The practice can have legitimate competitive purposes, such as blocking competitors' products, ensuring adequate supply of seasonal items, reintroducing products, or repositioning brands. The likely impact of the practice on current and future sales levels, however, should be adequately disclosed to avoid presenting a misleading picture of company sales.

In April 2005, the SEC settled a case with Coca-Cola concerning channel stuffing. According to the SEC, near the end of each reporting period between 1997 and 1999, Coca-Cola implemented an undisclosed practice in Japan in which Japanese bottlers were offered extended credit terms to induce them to purchase quantities of beverage concentrate the bottlers otherwise would not have purchased until a following period. Coca-Cola typically sells gallons of concentrate to its bottlers corresponding to its bottlers' sales of finished products to retailers. As a result, bottlers' concentrate inventory levels typically increase approximately in proportion to their sales of finished products to retailers. Because of Coca-Cola's practice, from 1997 to 1999 its Japanese bottlers' concentrate inventory levels increased at a rate more than five times greater than that of finished product sales to retailers. That pulled forward sales from subsequent periods and made it likely that Coca-Cola's bottlers would purchase less concentrate in the later periods.[16]

One potential red flag that may point to channel stuffing is an increase in shipments—usually accompanied by an increase in shipping costs—either at or near the end of a period. In such an instance, auditors may ask whether the goods were sold at steep discounts and then review customer contracts and side agreements for unusual discounts in exchange for sales and right-of-return provisions. They may also ask sales and shipping personnel about management's influence over normal sales channel requirements.

Customers offered deep discounts often purchase excess inventory, only to return it after the close of the period. The auditor may consider the amount of returns shortly after the close of a period compared with prior periods, as well as the margins on sales recorded immediately before the end of a reporting period.

Another potential red flag for channel stuffing may be signaled by increased commitments for offsite storage and subsequent increases in inventory reserves or inventory write-offs. Keep in mind that those inventory reserves may not be recorded until subsequent quarters or years.

Bill-and-Hold Transactions

These schemes represent another common method of bypassing the delivery requirement. As its name implies, a legitimate sales order is received, gets processed, and is made ready for shipment. However, the customer may not be ready, willing, or able to accept delivery of the product at that time. The seller holds the goods or ships them to a different location, such as a third-party warehouse, until the customer is ready to accept shipment. The seller, however, recognizes revenue immediately upon

[16] SA Rel. No. 8569; SEA Rel. No. 51565; AAE Rel. No. 2232 (April 18, 2005).

shipment. The auditor may consider whether the seller has met—or is seeking to circumvent—certain SEC criteria:[17]

- The risk of ownership has passed to the buyer.
- The buyer has made a fixed commitment in writing to purchase the goods.
- The buyer has requested the transaction on a bill-and-hold basis and has a substantial business purpose for doing so.
- Delivery must be fixed and on a schedule reasonable and consistent with the buyer's business purpose.
- The seller must not retain any specific obligations under the agreement.
- Ordered goods must be segregated from the seller's inventory and cannot be used to fill other orders.
- The product must be complete and ready for shipment.

In addition to these criteria, the SEC recommends that preparers of financial statements consider the date by which the seller expects payment and whether the seller has modified its normal billing and credit terms for this buyer, the seller's past experiences with and pattern of bill-and-hold transactions, whether the buyer takes the loss if the goods decline in market value, whether the seller's custodial risks are insured, and whether there are any exceptions to the buyer's commitment to accept and pay for the goods sold—that is, whether any contingencies have been introduced.[18]

Agreements that do not meet the aforementioned criteria may be considered potential bill-and-hold schemes, and auditors may take a close look at whether:

- Bills of lading are signed by a company employee rather than a shipping company.
- Shipping documents indicate excessive shipments made to warehouses rather than to a customer's regular address.
- Shipping information is missing on invoices.
- High shipping costs are incurred near the end of the accounting period.
- Large, numerous, or unusual sales transactions occur shortly before the end of the period.
- Current-year monthly sales have decreased from the previous year, possibly indicating the reversal of fraudulent bill-and-hold transactions in a previous period.

Confronted with those potential red flags, the auditor may inquire with management about bill-and-hold policies and interview customers with bill-and-hold arrangements. The auditor may also inquire with warehouse personnel about so-called customer inventories being held on the premises or in a third-party warehouse or shipped to another company facility. Finally, the auditor may ask shipping

[17] See U.S. Securities and Exchange Commission, "In the Matter of Stewart Parness," AAE Rel. No. 108 (August 5, 1986); see also Financial Accounting Standards Board, Statement of Financial Accounting Concepts No. 5, par. 84(a); see also SOP 97–2, par. 22.
[18] Id.

department or finance personnel if they've ever been asked to falsify or alter shipping documents.

If additional investigation is warranted, the auditor may review customer contracts to determine whether they comply with SAB 104. The auditor may also review underlying shipping documents for accuracy and verify the existence of transactions; compare shipping costs with those of prior periods for reasonableness; review warehouse costs and understand the business purpose of all warehouses or offsite storage owned or used by the company; confirm special bill-and-hold terms with customers, including transfer of risk and liability to pay for the bill-and-hold goods; and test reconciliation of goods shipped to goods billed.

The auditor may select a sample of sales transactions from the sales journal; obtain the supporting documentation and inspect the sales order for approved credit terms; compare the details among the sales orders, shipping documents, and sales invoices for inconsistencies; compare the prices on sales invoices against published prices; recompute any extensions on sales invoices; and tour the facility or warehouse and inquire of warehouse personnel about held customer products.

In September 2008, the SEC filed an action against two former accounting executives of Bally Technologies, Inc. for engaging in a fraudulent accounting scheme to artificially inflate the company's reported revenue and present misleading information to investors about the company's earnings. The SEC complaint alleged that from the fourth quarter of fiscal year 2003 through the second quarter of fiscal year 2004, Bally's former accounting executives fraudulently recognized revenue on bill-and-hold transactions, made misleading disclosures and omissions regarding revenue recognition, and made materially false statements to the company's outside auditors when they represented the transactions were proper under GAAP. According to the complaint, the improper bill-and-hold sales led to a 25 percent overstatement of Bally's reported earnings per share for the fourth quarter of fiscal 2003 and to 33 percent and 27 percent overstatements of Bally's reported quarterly EPS numbers in the first and second quarters of 2004, respectively.[19]

Early Delivery of Product

Companies may circumvent the SAB 104 delivery requirement in a variety of ways, including shipping unfinished or incomplete products to customers; shipping before customers are ready to accept products; shipping products to customers who have not agreed to purchase them, often called soft sales; recognizing the full amount of revenue on contracts whose services are still due; and recognizing the full amount of revenue on fees collected up front. Under SAB 104, income may not be recognized under these circumstances because delivery has not actually occurred. On the receiving end, customers often return the unfinished product or demand more work (or rework) before payment is rendered.

Auditors may seek evidence of such circumventions by comparing returns in the current period and prior periods, comparing shipping costs in the current period and prior periods, and comparing shipping costs as a percentage of revenue in the current period and prior periods. They may also scrutinize the sales contract:

[19] SEC Rel. No. 20738; AAE Rel. No. 2887 (September 24, 2008).

In relation to delivery, when must payment be made? Which party bears the risk of loss on shipment? The audit or investigative team may then compare these contract terms with the requirements of SAB 104 and other accounting literature.

To extend the inquiry beyond the financial area, the auditor may make broad inquiries among personnel in shipping, in sales, and in the warehouse, seeking answers to the following questions:

In shipping:

- Were shipments made earlier than normal?
- Is any inventory in the warehouse documented as shipped?
- Was inventory shipped to addresses other than customer sites?
- Is there inventory being held for certain customers?
- Is inventory ever sent to offsite storage facilities?
- Were there any adjustments to shipping dates?
- Are there any consigned goods, and if so, where are they?

In sales:

- Are any shipments planned for arrival ahead of the customer's required delivery date?
- How often do sales personnel pick up product and deliver it to customers?
- Are there sales personnel with excessive amounts of samples?
- Do sales personnel have warehouse access?

In the warehouse:

- Are there any misstatements in the amount of merchandise the company ships or receives?
- Has there been destruction, concealment, predating, or postdating of shipping or inventory documents?
- Has there been an acceleration of shipments before the end of the month or year?
- Have there been shipments to a temporary site or to holding warehouses before final shipment to customers' premises?
- Are there any other unusual, questionable, or improper practices?

But the auditors' work does not necessarily end there. To investigate further any suspicions of early delivery, auditors could compare the purchase order date with the shipment date and determine whether sales personnel are paid commissions based upon the sale of product or upon collection. They might inspect shipping documents for missing, altered, or incorrect information and review customer logs or e-mail correspondence for complaints that goods were shipped before the customer was prepared to accept them.

When auditors narrow the focus to certain personnel they suspect of participating in an improper revenue recognition scheme, they may look into whether these people have outside related business interests. To pursue this line of inquiry, auditors

can search public records on certain entities and individuals to determine whether shipments have been made to these outside business interests or their addresses.

Partial Shipments

Many companies recognize 100 percent of revenue on an order, even if their shipments are partial or incomplete. The delivery requirement may not have been met, however, if the unshipped amount is a substantial portion of the total order.

Consider the SEC's complaint against Merge Healthcare Incorporated in November 2009. The SEC's complaint alleges that the company engaged in fraudulent accounting practices that involved the improper recognition of revenue from sales on transactions that included promises of specified future software enhancements, sale contingencies, and transactions in which Merge failed to properly execute contracts or failed to properly deliver products in the same fiscal period in which Merge recorded revenue from those transactions or both.[20]

Auditing for partial shipments is similar to auditing for early product delivery. Auditors may look for numerous returns of incomplete products after the close of the period or for large, numerous, or unusual transactions occurring shortly before the end of the period. They may also consider examining invoices to determine whether all products ordered are listed and whether they were shipped or not. In the case of drop shipments, if such a shipment is partial, is the invoice to the customer also partial? Auditors may need to determine how the client ensures that all drop-shipped products are properly accounted for in the sales invoice process and also in payments received. Auditors may also consider reviewing customer complaints regarding incomplete shipments.

The auditor may inquire with management and sales personnel about policies and processes for billing partially filled orders. A review of shipping documents and a comparison to the sales journal may reveal what was booked as sales and what was actually shipped. And the auditor may want to talk to customers or review correspondence from them to determine whether there are complaints about partial shipments.

Contracts with Multiple Deliverables

Another common scheme is to ship product or equipment to customers that are not obligated to pay until the goods are accepted. Common customer-acceptance provisions include the seller's obligation to install and activate products after delivery, to conduct product testing, or to train personnel in product use. Acceptance typically requires a seller to fulfill such terms substantially before delivery is deemed to have occurred. If a contract requires the seller to provide such multiple deliverables, the delivery is not deemed complete unless substantially all elements have been delivered, and the sales revenue may be recognized only then.

In an assessment of whether revenue can be recognized before delivery of all required elements, the criterion under GAAP is whether the undelivered portion is

[20] AAE Rel. No. 3067 (November 9, 2009).

"essential to the functionality" of the total deliverable.[21] SAB 104 enumerates several factors that may be considered in determining whether remaining performance obligations are substantial or inconsequential.[22]

The SEC action against Intervoice, Inc. focused on improper revenue recognition in connection with contracts that had multiple deliverables. According to the SEC complaint, the company's CFO, Roy J. Graham, negotiated and approved transactions between Intervoice and its distributors that were each subject to significant, ongoing, post-transaction obligations and thus did not qualify for revenue recognition under Intervoice's policies or GAAP. The SEC alleged that, as to certain transactions, Graham agreed in advance to reconfigure the hardware and software products, or to substitute products of commensurate value, so it could better meet the needs of its distributors' ultimate end users, thereby precluding revenue recognition under GAAP. The complaint also alleged that Graham, in other transactions, requested distributors to take products in advance of their receiving orders from end customers, and agreed to allow the distributors to return the products without penalty if the end customers failed to purchase the products. According to the complaint, Graham failed to document these terms, and, in some cases, affirmatively misled Intervoice's external auditors by providing false information and documents.[23]

In addition to the general indicators listed earlier, auditors may consider confirming with major customers whether all services have been performed with respect to products purchased and received. For companies that use distributors for their products, auditors may seek to determine whether the company forces a predetermined listing of SKUs (stock-keeping units) on its distributors—even without an order. In such cases, there may be a culture of forcing product out to distributors to make the numbers. One of the symptoms of this condition is a rash of returns from the distributors in subsequent months. Auditors can ask whether such returns get processed in timely fashion.

IMPROPER ALLOCATION OF VALUE IN MULTIPLE-ELEMENT REVENUE ARRANGEMENTS

Multiple-element revenue arrangements are common in the software industry and in other industries in which sales of products are combined with sales of services. For example, a multiple-element arrangement might include the sale of computer software along with the sale of a software maintenance agreement and of services related to the installation and integration of the software products. Accounting rules may call for different revenue recognition treatments for each of these elements, as follows.

- Revenues allocated to the software product might be recognizable upon delivery, assuming the seller had no significant product-related continuing obligations.

[21] U.S. Securities and Exchange Commission, SAB 104 § II. Topic 13. A.3—Substantial Performance and Acceptance, Question 3.
[22] Id.
[23] SA Rel. No. 8815; SEA Rel. No. 55944; AAE Rel. No. 2621 (June 22, 2007).

- Revenues allocated to the maintenance agreement would usually be ratably recognizable over the term of the maintenance contract.
- Revenues allocated to services may be recognized as such services get provided. Thus, the timing and amounts of recognizable revenues depend on identifying the respective elements and understanding their accounting implications, and they thereafter depend on properly allocating the total sales price of the arrangement to such elements.

Both AICPA SOP 97–2, *Software Revenue Recognition,* and SAB 104 set forth rules for the allocation of revenues among the elements of a multiple-element arrangement. Essentially, such allocations must be based on the respective fair values of the elements, and these fair value estimates must be supported by verifiable objective evidence (VOE). The accounting rules do not permit mere reliance on stated—that is, list—prices, or on the prices agreed to by the parties to the multiple-element arrangement. The SEC's concern is that prices listed in a multiple-element arrangement with a customer may not be representative of the fair value of those elements because the prices of the different components of the arrangement could be altered in negotiations and still result in the same aggregate consideration. The issue was dealt with in EITF 00–21, *Accounting for Revenue Arrangements with Multiple Deliverables,* paragraph 4.[24]

Fraud can be introduced into the process of allocating fair values among elements within multiple-element arrangements in one or more of the following ways:

- Fabricating, altering, or otherwise manipulating VOE data.
- Mischaracterizing the terms or nature of the elements that require deferred or ratable recognition of their allocated revenues—usually, by attempting to minimize the significance and related values of such elements and thereby increasing the value assigned to elements for which revenues can be recognized immediately.
- Bifurcating the arrangement to make it seem as if the maintenance or services components were sold separately, at arm's length–negotiated prices stated in their bifurcated transactions, when in fact all of the subject elements were negotiated as a single deal and are interdependent.
- Misstating the prices at which the elements were planned to be sold—in the case of new products for which VOE is not yet available.
- Concealment or mischaracterization of the nature of up-front fees associated with deals. Under GAAP, many such fees are required to be recognized ratably over the term of the arrangement.

Up-Front Fees

Some companies collect payment in full up front for services provided over an extended period, such as in maintenance contracts. SAB 104 provides that up-front

[24] U.S. Securities and Exchange Commission, SAB 104 § II. Topic 13. A.3, Question 4, Answer 2; EITF 00–21 was updated by EITF 08–01, *Accounting for Revenue Arrangements with Multiple Deliverables,* issued 2008.

fees should generally be recognized over the life of the contract or the expected period of performance.

IMPROPER ACCOUNTING FOR CONSTRUCTION CONTRACTS

GAAP provides for contract revenue to be recognized by using either the percentage-of-completion or completed-contract method. The percentage-of-completion method applies only if management can reliably estimate progress toward completion of a contract.[25] When management cannot provide such estimates, GAAP calls for the completed-contract method, which requires the company to postpone recognition of revenue until the contractual obligations have been met.[26]

The percentage-of-completion method is often subject to abuse. Some companies use this method even if they do not qualify for it. Companies can artificially inflate revenue by increasing the costs incurred toward completion, underestimating the costs of completion, or overestimating the percentage completed. Accounting irregularities in this area involve:

- Misstatement of the percentage of completion either by intentionally mismeasuring such or by falsifying or manipulating engineering or cost accounting records or both
- Hiding cost overruns, which might require accrual as contingent losses and thus reduce profits related to the contract
- Misrepresenting the nature and collectability of cost overruns by falsely stating that such are add-ons, or contract amendments, that will be realized as additional revenue when in fact either they are not or they are subject to dispute with the customer

The auditor may start by selecting a sample of contracts and confirming their original contract price; total approved change orders; total billings and payments; details of claims, back charges, or disputes; and estimated completion date. Next, the auditor may determine whether all incurred costs are supported with adequate documentation detailing the nature and amount of expense, examining closely the estimated costs to complete. Do they seem reasonable after a review of estimates and a comparison with actual costs incurred after the balance sheet date? Are the underlying assumptions about estimated costs reasonable?

As further steps, the auditor may:

- Ensure that all contracts have been approved by appropriate personnel.
- Review unapproved change orders.
- Identify unique contracts and retest the estimates of cost and progress on the contract.

[25] See American Institute of Certified Public Accountants, Statement of Position (SOP) 81–1, par. 23.
[26] Id., par. 30.

- Test contract costs to verify that costs have been matched with appropriate contracts and that costs have not been shifted from unprofitable contracts to profitable ones.
- Verify that losses get recorded as incurred.
- Review all disputes and claims.
- Visit the construction contract site to view the progress of a contract.
- Interview project managers, subcontractors, engineers, and technical personnel to get additional information on the progress of an engagement and the assumptions behind the contract.

In 2003, the SEC filed a complaint involving financial fraud against several former officers of Analytical Surveys, Inc. (ASI), a company that provides computerized maps to customers under long-term contracts. According to the complaint, the company engaged in a fraudulent scheme that caused ASI's 1999 fiscal year revenue and net earnings to be materially inflated. The SEC alleged that ASI improperly recognized revenue on long-term contracts by directing employees to: (1) "finish contracts on indirect," whereby employees misallocated direct costs properly attributable to contracts to indirect, or overhead, accounts; (2) engage in "cost-shifting," where employees improperly shifted future direct costs from one contract to another, when the work performed related to the first contract and did not reflect progress on the second contract; and (3) improperly lower estimates of total direct costs on certain contracts or not increase cost estimates as necessary. According to the SEC, all of these methods were impermissible under the percentage-of-completion method for recognizing revenue used by ASI because GAAP requires that, under the percentage-of-completion method, estimated contract costs be periodically reviewed and revised to reflect accurate information.[27]

RELATED-PARTY TRANSACTIONS

We noted earlier that related-party transactions bear a higher risk of including sham transactions. Transactions between related parties are often difficult to audit because they are not always accounted for in a manner that communicates their substance and effect with transparency. The possibility of collusion always exists, given that the parties are, by definition, related. Internal controls, moreover, might not identify the transactions as involving related parties. While related-party transactions may involve improper revenue recognition, they may also involve other parts of the balance sheet or income statement.

An auditor may encounter related parties that are known to some members of the company, even if the relationships are not properly disclosed in the books and records. The auditor may inquire about an individual's outside business interests—and then try to determine whether they are properly disclosed—and the volume of transactions, if any, occurring between the entities. If certain entities are under scrutiny, the auditor may consider requesting a public records check of the entity to see whether there are indicators of undisclosed ties to particular individuals.

[27] SEC Rel. No. 18387; AAE Rel. No. 1886 (October 2, 2003).

Auditors may also focus on the relationship and identity of the other party to the transaction and on whether the transaction emphasizes form over substance. Common indicators of such related-party sham transactions include:

- Borrowing or lending either interest free or significantly above or below market rates
- Selling real estate at prices that differ significantly from appraised value
- Exchanging property for similar property in a nonmonetary transaction
- Loans with no scheduled terms for when or how the funds will be repaid[28]
- Loans with accruing interest that differs significantly from market rates
- Loans to parties lacking the capacity to repay
- Loans advanced for valid business purposes and later written off as uncollectible[29]
- Nonrecourse loans to shareholders
- Agreements requiring one party to pay expenses on the other's behalf
- Round-tripping sales arrangements
- Business arrangements in which the entity makes or receives payments of amounts at other than market values
- Failure to disclose adequately the nature and amounts of related-party relationships and transactions as required by GAAP[30]
- Consulting arrangements with directors, officers, or other members of management
- Land sales and other transactions with buyers that are marginal credit risks
- Monies transferred to or from the company from or to a related party for goods or services that were never rendered
- Goods purchased or sent to another party at less than cost
- Material receivables or payables to or from related parties such as officers, directors, and other employees[31]
- Discovery of a previously undisclosed related party
- Large, unusual transactions with one party or a few other parties at period end
- Sales to high-risk jurisdictions or jurisdictions in which the entity would not be expected to conduct business

When related-party transactions are detected or suspected, auditors have several places to start. They may search public records and conduct background

[28] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 45, *Related Parties* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 334), par. 3.
[29] American Institute of Certified Public Accountants, Practice Alert No. 95–3, *Auditing Related Parties and Related Party Transactions,* issued November 1995 (updated through July 1, 1999), par. 3, bullet 8. Superseded by the American Institute of Certified Public Accountants, *Accounting and Auditing for Related Parties and Related Party Transactions: A Toolkit for Accountants and Auditors* (December 2001).
[30] ASC 850–10-50, "Broad Transactions, Related Party Disclosures, Overall, Disclosure."
[31] See American Institute of Certified Public Accountants, *Accounting and Auditing for Related Parties and Related Party Transactions: A Toolkit for Accountants and Auditors* (December 2001).

investigations on customers, suppliers, other third parties, and other individuals to identify related parties and confirm the legitimacy of their businesses. (See Chapter 15.) They may do some data mining to determine whether transactions appear on computerized files. (See Chapter 17.) They may review documents of identified transactions to obtain additional information for further inquiry. And they may go on to any of the following steps and procedures.

- Search for unusual or complex transactions occurring close to the end of a reporting period.
- Search for significant bank accounting or operations for which there is no apparent business purpose.
- Review the nature and extent of business transacted with major suppliers, customers, borrowers, and lenders to look for previously undisclosed relationships.
- Review confirmations of loans receivable and payable for indications of guarantees.
- Review material cash disbursements, advances, and investments to determine whether the company is funding a related entity.
- Test supporting documentation for contracts and sales orders to ensure that they have been appropriately recorded.
- Discuss with counsel, prior auditors, and other service providers—to the extent confidentiality permits—the extent of their knowledge of parties to material transactions.
- Inquire whether management, owners, or certain individuals conduct business with related parties.
- Inquire about side agreements with related parties for right of return or contract cancellation without recourse.

Undisclosed related-party transactions are common. In some nations and industries, doing business with friends and relatives is commonplace. For global entities, even though there may be a requirement to disclose related-party transactions and business interests, there is no guarantee that that practice is being followed or even communicated at remote locations. Understand your client's industry and businesses. What may be sound policy in the handbook may not be practiced in some parts of the world.

REVENUE AND RECEIVABLE MISAPPROPRIATION

Of course, it is not the revenue or receivable that is misappropriated; it is the cash that businesses ultimately collect. While virtually any asset can be misappropriated, more than 90 percent of asset misappropriation schemes involve the taking of cash.[32] Cash is misappropriated both as it gets paid to the company—generally, sales receipts or receivables collections—and as it gets paid out by the company in

[32] See American Institute of Certified Public Accountants, *Accounting and Auditing for Related Parties and Related Party Transactions: A Toolkit for Accountants and Auditors* (December 2001).

fraudulent disbursements involving primarily payables, payroll, and employee expense reimbursement. Here we focus on the taking of cash receipts in the revenue cycle.

While many frauds begin on the balance sheet, many educated fraudsters attempt to move that fraud to the income statement for two reasons. First, balance sheet accounts may be subject to more scrutiny by auditors than are income statement accounts. Second, after at most 12 months, the income statement accounts will be closed out to one of the largest numbers on the balance sheet—retained earnings—never to be reviewed again. Fraudsters often attempt to hide the theft in either a large expense line item in which the amount stolen will be immaterial or by dispersing the theft among many expense line items so that it will not be material to any single line item.

Most frauds perpetrated in this manner are not the subjects of audit programs because there is little risk of material misstatement. While money was stolen, it was expensed, and the only risk of financial statement misstatement is misclassification on the income statement. Strange as it may sound, the financial statements are likely to be presented fairly and in accordance with accounting standards. It is only when misappropriations like these get hidden on the balance sheet that they become problematic from the standpoint of financial statement materiality. In such cases, they need to be written off, which is exactly what the fraudster may have done to disguise the activity rather than to correctly account for the transactions. Whatever the motive, an uncollectible receivable write-off *is* the correct accounting.

Revenues

Defalcation involving revenues has to do with cash, not credit, sales. These could be retail sales or purchase orders accompanied by payment. Payment could be in the form of either cash or check. When the incoming payment is in the form of a check, the perpetrator will need to alter the check (see the following discussion on check tampering) so that it becomes payable to himself or for his benefit, or he will need to endorse the check secondarily.

Revenues can be misappropriated through skimming or larceny. *Skimming* is the term used when cash receipts are taken before they are recorded in the accounting system; the sale therefore never gets reflected in the company's books and records. In 2003, at least eight Southwest Airlines employees were accused of misappropriating more than $1.1 million by a variety of skimming techniques. In one method, a ticket counter worker saved an old ticket that may have been voided. The unmarked ticket was then sold to a cash-paying customer, and the employee pocketed the money.

Larceny is the term used when the cash receipts are taken after being recorded in the accounting system; the sale is therefore reflected in the company's books and records. In the case of larceny, if the debit entry to the sales entry is cash, cash will not balance. More often, the debit entry will be to receivables so that cash remains in balance.

Analytical procedures represent one of the most effective detection techniques for asset misappropriation schemes, and the more disaggregated the review, the better. The analytical relationship that will reveal such a defalcation depends, of course, on the way the defalcation was perpetrated and recorded. Analytics related to possible revenue schemes include:

- Trend revenue on a monthly basis over time for evidence of a downward or flat trend when an upward trend was expected.
- Cash that is decreasing in relation to total current assets.
- Cash that is decreasing in relation to credit sales.
- A decrease in sales accompanied by an increase in cost of sales.
- A current ratio that has decreased significantly from prior periods.
- Cash collections that are significantly less than reported revenues.
- Trend revenue by employee over time if multiple individuals handle revenue payments.
- Trend gross profit: If the sale is made but not booked, gross profit will be reduced.
- Trend payments on accounts receivable: A decreasing trend in payments indicates receivables will grow and age.
- Significant write-offs in the current period compared with the previous period.
- Trend accounts receivable write-offs: If the sale is made and booked as a receivable, it may be written off rather than allowed to age and be included in collection efforts.
- Analysis of credit memos.

Customer complaints may also be potential red flags for a hidden-revenue misappropriation scheme. If a customer payment is converted but the sale is made and recorded as a receivable, customer complaints will occur if the company attempts to collect a receivable when the customer paid at the time of order. Lapping receivables, as described later, are attempts by the fraudster to conceal these thefts. A gap in issued invoice numbers is another possible red flag. In one example involving a cash-intensive business, customer tickets—essentially, invoices—were not included in submitted paperwork, and the associated cash receipts from these customers were neither reported nor submitted. This resulted in gaps in customer ticket numbers, and these gaps were noticed and made part of the detection process. Other risk factors pointing to possible point-of-sale or point-of-cash-collection misappropriation schemes are:

- Lack of segregation of duties among the sales, receipts, and recording functions
- Poor controls over the completeness of the recording of sales
- A sharp increase in the average length of time that customer cash receipts are maintained in an account before being applied to the customer's outstanding balance
- Periodic, large, or numerous debits or other write-offs to aged accounts
- Recorded customer complaints regarding misapplication of payments to customer accounts
- Forced account balances, such as overstatements of cash balances, that are made to match the accounts receivable balance
- Numerous or significant reversing entries or other adjustments that have caused the books or the register to reconcile to the amount of cash on hand
- Large or numerous debit adjustments to aged receivable accounts
- Finally, journal entries made to cash, which are rare and would suggest the need for further scrutiny

Receivables

As with revenues, cash remittances related to accounts receivable may be taken both through skimming and through larceny. A larceny of receivables—that is, receivables taken after the collection of the receivables has been booked—results in cash that doesn't balance. As a result, receivables larceny schemes are less common than receivables skimming schemes. A receivables skimming scheme, however, ultimately results in customer complaints when the company tries to collect a receivable that has already been paid. Many fraudsters use a lapping scheme (described in detail later in this chapter) to avoid or delay detection of the fraud. A lapping scheme starts with a skimmed receivable, whereby the cash paid to relieve the receivable is stolen and not recorded. To prevent the receivable from continuing to age, a subsequent cash payment from a different customer is recorded as a payment in place of the one converted. This crediting of one account with payment by another account must continue on an ongoing basis to avoid detection of the scheme. Each additional receivable stolen or used for covering another customer's account must be covered by subsequent receipts from other customers for the scheme to continue.

If a receivables scheme is suspected, confirmations of receivables balances will have heightened importance. It may be appropriate also to confirm balances orally and to request copies of canceled checks, front and back, from certain customers. The reverse side of a canceled check may show secondary endorsements from the company to the perpetrator, or to a shell company incorporated by the perpetrator, or to an accomplice. While many banks will not accept at the teller window such checks with secondary endorsements, if such checks are deposited through the use of an ATM or night deposit, they are not typically reviewed for secondary endorsements. A review of customer checks may also reveal that the checks—typically, the payee information—were altered, thereby allowing the perpetrator to negotiate the check.

Fictitious Sales

A common technique is to create fictitious orders for either existing or fictitious customers. Recording a fictitious sale in a company's books and records is as simple as posting a credit to the general ledger. False supporting documentation is created to support the nonexisting sales or services never rendered. However, the fictitious account receivable that must be created in this scheme will never be collected. Eventually, this uncollected account receivable will age; that is, it will grow older and become 30, then 60, then 90, and eventually, 120 days—and more—past due. Long-past-due receivables attract attention; they need, therefore, to be concealed.

One means of doing so is simply to write off the receivable in some future period. This method is based on the fraudster's expectation that future revenues and profits will be sufficient to permit such a write-off; thus, it is a form of timing irregularity. However, evidence of the original, fictitious transaction, as well as of the subsequent write-off, still remains in the books and records, and the reason for the write-off may be questioned. Another way to conceal the fraudulent transaction is to charge it to the account called Sales Returns and Allowances, with the explanation that the customer returned the products for some plausible reason. However, this concealment approach requires that:

- The allowance balance be sufficiently large to absorb such a charge, permitting reprovision of the allowance over future periods.
- The effect of the charge does not raise questions about the adequacy of the allowance and sales returns provisions recorded in prior periods.
- No one challenges the circumstances of the transaction or the subsequent product return.

Possible Red Flags for Fictitious Receivables

- Unexpected increases in sales and corresponding receivables by month at period end
- Large discounts, allowances, credits, or returns after the close of the accounting period
- Large receivable balances from related parties or from customers with unfamiliar names or addresses or that have no apparent business relation to the business
- Receivable balances that increase faster than sales
- Organizations that pay commissions based on sales rather than the collection of the receivable
- Increased receivable balances accompanied by stable or decreasing cost of sales and corresponding improvement in gross margins
- Lengthening of aging of receivables or granting of extended credit terms
- Excessive write-offs of customer receivable balances after period end
- Re-aging of receivables
- Excessive use of an account called either *Miscellaneous* or *Unidentified Customer*
- An increased trend of past-due receivables
- Lack of adequate controls in the sales and billing functions

Lapping

Yet another way to conceal the transaction is a form of kiting, or lapping, wherein collections from a legitimate customer transaction are diverted and misapplied to pay off the fictitious receivable balance. For example, the perpetrator steals the payment intended for customer A's account. When a payment is received from customer B, the thief credits it to A's account. And when customer C pays, that money is credited to B. Of course, this exposes the legitimate receivable to noncollection because it is unlikely that the legitimate customer will pay twice for the same purchase. Therefore, subsequent diversions and misapplications of collections must be done over and over again. Lapping tends to increase at exponential rates and is often revealed because the employee is unable to keep track of or obtain additional payments to cover up the prior skimming.[33]

Lapping, like all forms of kiting, is plagued by complexity and usually requires the notorious so-called "second set of books" to track all of the diversions and misapplications and keep a record of which legitimate receivables need to be covered by

[33] Joseph T. Wells, "Lapping It Up: A Skimming Method Doomed to Failure over Time," *Journal of Accountancy* (February 2002): 73–75.

which misapplied collections. Unless a future reckoning is made by eventually writing off some receivable balance(s) in the amount of the original fictitious receivable, this type of scheme becomes a perpetual motion device, which at some point must grind to a halt. Compounding this obvious problem is the tendency of these kinds of frauds to grow through more and more fictitious entries requiring more and more deceptions to conceal their existence.

Redating

There is yet another type of scheme wherein the receivable is redated to a more current date. This keeps the amount from being captured in the bad debt reserve. However, the receivable is still at risk of being selected by the auditors for confirmation.

Such schemes can often be detected by the same methods used in detecting premature-revenue-recognition schemes. Auditors may look closely at significant revenue adjustments at the end of the reporting period, unexpected increases in sales by month at period end, customers with unfamiliar names or addresses or with no apparent business relationship with the company, increased sales accompanied by stagnant or decreasing cost of sales and corresponding improvement in gross margins, evidence of the re-aging of receivables to keep fictitious amounts from attracting attention as they age, unusual charges to the Sales Returns and Allowances account, improvement in bad debts as a percentage of sales, and a decrease in shipping costs compared with sales.

Fictitious revenue schemes tend to be relatively easy to investigate, once detected. The audit team may focus on accounting personnel to determine whether revenues are being recorded outside the normal invoicing process or standard monthly journal entries, whether journal entries have adequate and genuine supporting documents, and whether accounting personnel have been pressured to make or adjust journal entries or to create false invoices for existing or fictitious customers.

The auditor may also ask sales or shipping personnel whether they have noted with no reasonable explanation any unusually high levels of sales or shipments to customers or have noted any significant sales or shipments to unfamiliar new customers.

INFLATING THE VALUE OF RECEIVABLES

Inflating the value of legitimate receivables has the same impact as creating fictitious ones. GAAP requires accounts receivable to be reported at net realizable value—the gross value minus an estimated allowance for uncollectible accounts.[34] GAAP also requires companies to estimate the uncollectible portion of a receivable, and the preferred method is either to record periodically the estimate of uncollectible receivables as a percentage of sales or of outstanding receivables or to use a calculation based on the aging of outstanding receivables.

[34] See American Institute of Certified Public Accountants, *Accounting and Auditing for Related Parties and Related Party Transactions: A Toolkit for Accountants and Auditors* (December 2001).

Under the allowance method, bad debt provisions are recorded on the income statement as a debit to bad debt expense and as a credit to allowance for doubtful accounts on the balance sheet contra-receivable account. When all or a portion of the receivable becomes uncollectible, the uncollectible amount is charged against the allowance account. When receivables are recorded at their true net realizable value, the recording of a bad debt provision decreases accounts receivable, current assets, working capital, and, most important, net income.

Companies may circumvent these rules by underestimating the uncollectible portion of a receivable. This artificially inflates the value of the receivable and records it at an amount higher than net realizable value. The overvaluing of receivables also serves to understate the allowance account, such that the provision is insufficient to accommodate receivables that in fact become uncollectible.

A related scheme involves not writing off or the delaying of the write-off of receivables that have, in fact, become uncollectible. These schemes usually are relatively easy to execute, given the subjectivity involved in estimating bad debt provisions. To investigate these possibilities, auditors review and understand the provision and determine its reasonableness by asking management and accounting personnel to explain the reasoning behind the amount.

Among the potential red flags that may surface are minimum bad debt provisions or reserves that appear to be inadequate in relation to prior periods, a history of extending payment terms to customers with limited ability to repay, a history of inadequate reserves for uncollectible receivables, deteriorating economic conditions or declining sales, deteriorating accounts receivable days outstanding, untimely or irregular reconciliations, net receivables (net of the allowance for a doubtful account) that are increasing faster than revenues, uncollectible accounts that have been on the books for extended periods but have not been written off, and recorded disputes with a customer that may potentially threaten the company's ability to collect. If auditors do identify some red flags, they may consider using some or all of the extended audit procedures discussed next.

EXTENDED PROCEDURES

Their suspicions aroused, auditors may consider a number of extended procedures, which include but need not be limited to the following:

- Send confirmations to or inquire with customers that may be associated with suspicious transactions.
- Perform alternative procedures for confirmations not returned or returned with material exceptions, such as including a blank line on which the customer must list the amount of pending returns or consigned inventory or both.
- Review journal entries and supporting documentation and verify their accuracy.
- Identify amount of returns in subsequent periods.
- Identify sales that got reversed in the subsequent period.
- Inquire of sales and credit department personnel about changes in credit policies, reserve rates, or bad debt expense policies.
- Inquire about any pressure to grant credit to customers of questionable credit quality or to extend payment terms.

- Research publicly available information to verify the existence and legitimacy of customers. Follow-up visits to listed sites may also be appropriate.

In situations in which fraudsters attempt to tamper with and corrupt the receivables confirmation process, fraudsters may try to cover their tracks in one or more of the following ways:

- Talking the auditors out of confirming receivables by arguing:
  - The response rate is too low. So why not just review subsequent collections? Or perform some kind of overall analysis of receivables' aged balances? Or just review documentation of sales transactions, such as invoices and purchase orders?
  - Confirmations bother our customers.
  - Customer ABC Corp. is unable to confirm overall balances; they can confirm only individual invoices, and it is difficult or impossible for us to match our invoices to their invoice references, so let's call the whole thing off.
- Falsifying the population records—such as the accounts receivable subsidiary ledger—to exclude the fictitious balances, thus preventing them from being confirmed. This approach also requires manipulating the data file so that totals include the amounts of the balances that were excluded, which in turn must depend on the auditor's not footing, or totaling, the subsidiary ledger's individual line items either manually or by use of an automated test program.
- Intercepting either the confirmations or the responses—and, in the latter case, altering the response. This in turn requires either or both of the following:
  - Collusion with someone at the party being confirmed
  - Theft of or tampering with the mail—outgoing or incoming
- Deceiving the party being confirmed, such as by contacting such party, alerting the party to the confirmation request being sent, and telling a lie, like: "The balance was inadvertently stated as $X, when in fact it should have been $Y. Just ignore the confirmation and don't respond to it or any subsequent inquiries. And if you have any questions, don't call the auditors; call me."
- Lying to the auditors after the fact by misrepresentations along these lines:
  - The customer is wrong. Here is all of our documentation of the transaction. The customer obviously made a mistake.
  - The customer is right. The customer did pay that balance, and we inadvertently posted the collection to the wrong account. (This requires undoing some other misapplication of collections and hoping the auditors do not follow up, by confirmation, with that customer balance.)
  - The customer is right. We improperly posted the original sales transaction, which should have been recorded to customer XYZ Corporation and not ABC Corporation. (This also depends on the auditor's not following up by confirming that balance with XYZ Corporation.)

Obviously, the least problematic way to corrupt the confirmation process is to alter the population from which any confirmation audit sample is to be drawn. Just as obviously, maintaining the fiction surrounding the original falsified revenue and receivable entries recorded in the general ledger also requires the creation of accompanying fraudulent documents and records, including:

- A fictitious invoice, purchase order, and delivery receipt
- Fictitious shipping documents and fictitious correspondence such as documentation of negotiation of the fictitious arrangement
- Fictitious entries to the general and subsidiary ledgers; to any applicable sales journal; to any inventory stock ledger, if applicable; and to any shipping record
- Fictitious collections records
- If necessary, fictitious aged accounts receivables schedules and reports

Carrying out this scheme could be hard work for just one person. For that reason, any serious fraud scheme of this type usually requires collusion by others such as revenue accountants, the manager in charge of revenue accounting, the general ledger accountants, accounts receivable subsidiary ledger accountants, or the accountant responsible for cash collections and their application to receivables balances.

ROUND-TRIPPING

Round-tripping is another approach to overstating revenue. It consists of the recording of transactions between companies and from which transactions there are no economic benefits to either company. For example, a company provides a loan for a customer so the customer can purchase product with no expectation that the customer will repay the loan. Such transactions are deemed completed for the sole purpose of inflating revenue and creating the appearance of strong sales.

Indications of round-trip-revenue frauds are:

- Complexity in the structure and rationale of the transaction
- Concealment of the true sources and uses of funds exchanged in the arrangement
- Attempts to disassociate the subject transaction(s) from other transactions on which the subject transaction(s) actually is (are) dependent
- Mischaracterization of the true relationships and rights and obligations among the parties

In 2002, the SEC began investigating the way in which Qwest Communications International and certain competitors, including Global Crossing, accounted for sales of fiber-optic capacity and whether it was proper for the company to recognize the revenue immediately.[35] Qwest sold capacity on its fiber-optic network to carriers and also purchased capacity from them. In each deal, both companies recognized revenue from capacity swaps and also what are known as indefeasible rights of use (IRUs), which allow another carrier or company unfettered use of the capacity over a long period of time. In some cases, the amounts of the sale and purchase were almost identical. According to the SEC, Qwest booked the revenue from these sales all at one time instead of deferring part of it over many years, although GAAP requires companies to record the revenue generated by an IRU over the time of the contract.

[35] SA Rel. No. 8295; SEA Rel. No. 48559; AAE Rel. No. 1879 (September 29, 2003).

The SEC concluded that the effect was to boost Qwest's revenue by $1 billion in 2001 and $465 million in 2000.[36]

Since most round-tripping transactions involve companies in the same line of business, an auditor may want to review a list of the company's significant customers. If a customer is in the same line of business, the auditor may want to scrutinize the transactions for evidence of round-tripping. The auditor may also want to review the vendor list and compare it with the customer list. A company whose name appears on both lists might also be a sign of round-tripping. Intermediaries are sometimes used in such transactions as a way of masking the activity. For this reason, caution is warranted as to companies named on both lists that do not appear to be customers or vendors. Round-tripping often occurs between related parties, and so the auditor might want to also scrutinize related-party transactions.

Clearly, companies determined to recognize revenue improperly have a wide range of techniques. Always keep in mind that reasonable assurance of payment is basic to revenue recognition. Some companies circumvent this by recognizing the full amount of revenue even though the customer has for some reason disputed payment. Auditors may determine which receivables are in dispute and, if necessary, confer with the company's legal counsel to assess whether collection of the revenue is sufficiently certain to be able to be properly recognized.

IMPROPERLY HOLDING OPEN THE BOOKS

Improperly holding open the books beyond the end of an accounting period can enable companies to record additional end-of-period sales that have been otherwise invoiced and shipped after the end of a reporting period. Standard cutoff testing often discloses such schemes, but skill in detecting manipulation of information systems may be required. Direct inquiry of accounting personnel, billing clerks, and warehouse personnel may assist in determining whether the books have been held open past the end of the period. Computer forensics can also be used to ferret out such schemes.

In September 2004, the SEC filed a complaint against Computer Associates International that alleged that the company kept its books open to record revenue from contracts executed after the quarter ended in order to meet Wall Street quarterly earnings estimates. During the period from at least January 1, 1998, through September 30, 2000, Computer Associates prematurely recognized over $3.3 billion in revenue from at least 363 software contracts that Computer Associates, its customer, or both parties, had not yet executed, in violation of GAAP. For example, in the first, second, third, and fourth quarters of FY2000, respectively, Computer Associates allegedly inflated its properly recorded revenue by approximately 25 percent, 53 percent, 46 percent, and 22 percent by improperly including prematurely recognized revenue. The complaint alleges that company executives held Computer Associates' books open for several days after the end of each quarter to improperly

[36] Id.

record in that quarter revenue from contracts that were not executed by customers or Computer Associates until several days or more after the expiration of the quarter.[37]

Companies may also hold open the books to capture additional shipments and thus recognize revenue prematurely. In one matter, forensic accounting investigators obtained the electronic daily sales summary used to report flash results to headquarters at the end of each month and quarter. While nothing untoward was evident from the printed version of the schedule, the entry for the last day of each accounting period could be seen in the electronic version to be composed of a sum of individual entries. When asked about these entries, the division controller's secretary promptly explained that each item in the sum represented the shipments on an additional day included in the accounting period. She explained that she needed this record of how many days the quarter had been held open because the company would never condone mistakenly reporting the same sale twice! She went on to say that she had to start the next month with the "correct" date.

CONSIGNMENTS AND DEMONSTRATION GOODS

As noted previously, SAB 101 prohibits revenue recognition from consignment arrangements until completion of the actual sale. The same criterion applies to products delivered for demonstration purposes.[38] In a typical consignment arrangement, neither title nor the risks and rewards of ownership pass from the seller to the buyer. Consignment sales and products shipped for trial or evaluation are examples of contingent events that must be converted into actual sales before revenue can be recognized.

Careful consideration is recommended regarding the terms, facts, and circumstances of any agreement in which the buyer has the right to return the product to determine whether:

- The buyer does not pay the seller at the time of sale, and the buyer is not obligated to pay the seller at a specified date or dates.
- The buyer does not pay the seller at the time of sale but is instead obligated to pay at a specified date or dates, and the buyer's obligation to pay is contractually or implicitly excused until the buyer resells the product or subsequently consumes or uses the product.
- The buyer does or does not have an obligation in the event of theft or physical destruction or damage of the product; in other words, there is no transfer of risk.
- The seller provides all economic substance for the sale transaction through credit and right-of-return transaction terms.
- The seller has significant obligations for future performance to bring about repurchase of the product by the buyer.
- The product is delivered for demonstration purposes.[39]

---

[37] ESC Rel. No. 18891; AAE Rel. No.2106 (September 22, 2004).
[38] U.S. Securities and Exchange Commission, SAB 101 § II. Topic 13. A.2, Question 2.
[39] Id.

SUMMARY

Financial reporting fraud involves revenue and receivable accounts more often than any other type of fraudulent scheme. This is unsurprising given the revenue and growth focus of modern securities markets. Theft of cash, often during the collection process from customers, is the most common form of asset misappropriation. This, too, is unsurprising given that cash is an easily converted asset. Based on these factors, SAS 99 recognizes that material misstatements due to fraudulent financial reporting often result from an overstatement of revenues (for example, through premature revenue recognition or recording fictitious revenues) or an understatement of revenues (for example, through improperly shifting revenues to a later period). The auditor should therefore ordinarily presume that there is a risk of material misstatement due to fraud relating to revenue recognition.[40]

[40] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 316), par. 41.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 23

Financial Statement Fraud: Other Schemes and Misappropriations

Jonny J. Frank, David Jansen, and Michael Carey

Alongside the well-populated universe of improper revenue recognition schemes is a parallel universe of asset overstatement and liability understatement, in which fraudulent schemes also abound. A direct relationship exists between overstatement of assets and understatement of liabilities and expenses, as many recent financial frauds have demonstrated. Among the most common financial statement frauds in these areas are the following: manipulating management estimates; creating fictitious assets; manipulating the balances of legitimate assets, particularly investments, with the intent to overstate value; understating liabilities or expenses; failing to record or deliberately underestimating accrued expenses, environmental or litigation liabilities; restructuring reserves; misstating intercompany expenses; and manipulating foreign exchange transactions.

ASSET MISSTATEMENTS

Aside from accounts receivable, discussed in Chapter 22, inventory is one of the most misstated assets, and cash is the most often misappropriated. Among the other types of assets commonly misstated are investments, fixed assets, leased assets, research and development costs, software development costs, advertising costs, and interest costs. Very often, the easiest way for a fraudster to accomplish his objective is to manipulate management estimates of value, reserves, or provisions.

Inventory Schemes

The first report by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) found that fraudulent asset valuations accounted for nearly half of the cases of financial statement fraud,[1] while misstatements of inventory accounted for more than half of asset valuation frauds. Generally, when inventory is

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Report of the National Commission on Fraudulent Financial Reporting* (1987), 103.

sold, the amounts are transferred to cost of goods sold and included in the income statement as a direct reduction of sales. An overvaluation of ending inventory understates cost of goods sold and in turn overstates net income. Inventory schemes generally fall into three categories:

1. Artificial inflation of the quantity of inventory on hand
2. Inflation of the value of inventory by postponing write-downs for obsolescence, manipulating the unit of measurement to inflate value, underreporting reserves for obsolete inventory (especially in industries whose products are being updated or have a short shelf life), and changing between inventory reporting methods
3. Fraudulent or improper inventory capitalization

Among the indicators of such schemes are a gross profit margin higher than expected, inventory that increases faster than sales, inventory turnover that decreases from one period to the next, shipping costs that decrease as a percentage of inventory, inventory as a percentage of total assets that rise faster than expected, decreasing cost of sales as a percentage of sales, cost of goods sold per the books that does not agree with the company's tax return, falling shipping costs while total inventory or cost of sales has increased, and monthly trend analyses that indicate spikes in inventory balances near year-end.

Inflation of Inventory Quantity The simplest way to overstate inventory is to add fictitious items. Companies can create fake or fictitious journal entries, shipping and receiving reports, purchase orders, and quantities on cycle counts or physical counts. Some companies go so far as to maintain empty boxes in a warehouse. In one inventory scheme, the extra boxes were filled with bricks that matched the company's product in size and weight so that the fraud would not be discovered during the physical inventory count observation if an auditor happened to pick up, move, or weigh individual boxes or pallets.

The most effective way for the auditor to confirm inventory quantities and identify valuation issues is to observe the client's physical inventory, particularly when an inventory count is being performed. Generally Accepted Auditing Standards say, "It is ordinarily necessary for the independent auditor to be present at the time of count and, by suitable observation, tests, and inquiries, satisfy himself respecting the effectiveness of the methods of inventory-taking and the measure of reliance which may be placed upon the client's representations about the quantities and physical condition of the inventories."[2] When auditors are not satisfied with the client's inventory procedures and methods, they must physically count the inventory themselves and test the transactions.[3] When inventory is stored outside the company site, such as in public warehouses, auditors may conduct additional procedures to confirm balance. Those additional procedures may include surprise visits to the offsite locations as well as inquiries to identify all offsite storage locations.

[2] American Institute of Certified Public Accountants, Statement on Auditing Standards (SAS) No. 1 § 331 (codified in AICPA Professional Standards—U.S. Auditing Standards—AU § 331), par. 11.
[3] Id.

Among companies that have been found to have engaged in fictitious inventory schemes are Crazy Eddie, McKesson & Robbins, and ZZZZ Best, but perhaps the best-known inventory fraud was the salad oil swindle of the 1960s.[4] An entrepreneur named Anthony DeAngelis rented petroleum tanks in New Jersey and filled them with seawater, with the exception of just one smaller tank, nested inside a larger tank, which he filled with salad oil. He was able to persuade auditors and lenders, including American Express, that the tanks contained more than $100 million in vegetable oil because the opening for the dipstick went into the little oil tank. DeAngelis used warehouse receipts confirming the existence of the huge inventory of vegetable oil as collateral for $175 million in loans. Using the borrowed funds to speculate on vegetable oil futures in the commodities market, DeAngelis was doing nicely until vegetable oil prices took a dive and he lost everything. The embarrassed lenders soon discovered the truth: They now owned tanks of seawater. The equally embarrassed auditors realized that DeAngelis and his accomplices had successfully misled them.

An auditor may consider operational factors to investigate suspicions of fictitious inventory. As in the salad oil case, this includes inventory that cannot be easily inspected physically or that is stored in unusual locations. It includes, as well, the following:

- Unsupported inventory, cost-of-sales, or accounts payable journal entries.
- Unusual or suspicious shipping and receiving reports.
- Unusual or suspicious purchase orders.
- Large test count differences.
- Inventory that does not appear to have been used for some time.
- Large quantities of high-cost items in summarized inventory.
- Unclear or ineffective cutoff procedures or inclusion in inventory of merchandise already sold or for which purchases have not been recorded.
- Adjustment of entries that have increased inventory over time.
- Material reversing entries to the inventory account after the close of the accounting period.
- Inventory that is not subject to a physical count at year-end.
- Sales that are reversed and included in inventory but not counted in the physical observation: For example, a company "accidentally" delivers a product to a customer, tells the customer it was a mistake, and requests that the customer send the product back.
- Excessive intercompany and interplant movement of inventory with little or no related controls or documentation.

Keeping that salad oil dipstick in mind, we can see that even physical observation is not foolproof. A company can perpetrate fraud by:

- Following the auditor during the count and adding fictitious inventory to the items not tested
- Modifying the count sheets

[4] See Norman C. Miller, *The Great Salad Oil Swindle* (New York: Howard McCann, 1965).

- Obtaining advance notice of the timing and location of inventory counts so that it can conceal shortages by shifting inventory from locations not visited
- Entering on count sheets, cards, or scanners additional quantities that do not exist—even adding a digit in front of the actual count
- Falsifying shipping documents to show that inventory is in transit from one company location to another
- Falsifying documents to show that inventory is located at a public warehouse not controlled by the company
- Including as part of the inventory count certain consigned items or items held for customers

What can an auditor do in the face of such determined inventory fraud? Auditors may consider company policy on both frequency of and procedures for inventory counts, compare any dollar adjustments on the books with physical counts and explore the reasons for significant differences, ask whether all inventory shrinkages have been reported, observe inventory at third-party locations, conduct physical inventories at multiple locations on the same day, and make test counts *from* the count sheets *to* the physical inventory.

Inflation of Inventory Value Generally Accepted Accounting Principles (GAAP) require that inventory be reported at cost or market value, whichever is lower. Companies inflate inventory value for a variety of reasons, including the use of inventory as collateral for financing. Inflating inventory value achieves the same impact on earnings as does manipulating the physical count. Management can accomplish this simply by creating false journal entries designed to increase the balance in the inventory account. Another common way to inflate inventory value is to delay the write-down of obsolete or slow-moving inventory because a write-down would require a charge against earnings.

In response, auditors may gain an understanding of the items in inventory and their life cycles, particularly in the context of the relevant industry. During physical observation of the inventory, the auditor may look for and ask about older items that might be obsolete. In industries with changes in product lines or technology or with rapid declines in sales or markets, few or no write-downs to market or no provisions for obsolescence may be possible red flags.

When an inventory valuation problem is suspected, the auditor may ask accounting personnel about inventory pricing policy and how they identify net realizable value markdowns. The auditor may ask management, accounting, and finance personnel about the company's historical patterns and whether there has been overvaluation. The auditor may determine whether accounting personnel have been asked to delay inventory write-downs because of obsolescence or other factors. In addition to looking for old or obsolete merchandise in the warehouse, the auditor may ask whether any stock is slow moving or damaged. The auditor may inquire about whether any stock is being sold below cost. And the auditor may step back, look broadly at the industry, and ask industry experts whether the products are salable and at what cost.

Fraudulent or Improper Inventory Capitalization Companies sometimes seek to inflate inventory by capitalizing certain expenditures associated with inventory, such

EXHIBIT 23.1 Irregularities in the Inventory/Cost of Sales Equation

Cost of sales is computed as:		Irregularity
Purchases	XX	Decrease
+ Direct Labor	XX	Decrease
+ Overhead Costs	XX	Decrease
	XX	
+ Beginning Inventory	XX	Decrease
− Ending Inventory	(XX)	Increase*
Cost of Sales	XX	Net Decrease

*Increased ending inventory is achieved by overstating the count of goods on hand, by overstating the value assigned to such goods, or by understating the amount of reserves or write-downs.

as sales expenses or general and administrative overhead. Amounts that are actually expenses are improperly reported as additions to the asset balance, thus artificially increasing inventory value.

Auditors and forensic accounting investigators may need to be familiar with both the company's capitalization policies and industry practice. If past accounting policies have been aggressive on capitalization, the auditor may have reason to investigate further. Finally, the auditor may look for changes to standardized cost amounts that increase the amounts capitalized to inventory.

Overstating ending inventory for the purpose of understating costs of goods sold for the period has one main drawback: That period's ending inventory becomes the next period's beginning inventory balance. Thus, any such overstatement will cause the next period's cost of sales to increase by that amount. This usually means that inventory frauds must be recurring and must grow in size, unless their purpose is just to shift costs from one accounting period to the next. (See Exhibit 23.1.)

Investment Schemes

Fraudulent investment schemes provide another method for a company to overstate assets by creating fictitious investments or deliberately overvaluing existing ones.

Auditors may gain an understanding of and familiarity with all of a company's investments and understand their classifications so they can spot possible red flags that may signal potential fraudulent practices. The auditor may be aware of the current market status of all investments and confirm that the books and records reflect all increases or decreases in such status. In addition, the auditor may question all classifications of securities to ensure that they are classified in a consistent manner rather than solely to recognize gain or to forgo recognizing loss.[5] The auditor may also be wary of losses on securities held as available for sale that are accumulating in the other comprehensive income account. The company must eventually take a charge for these losses—either through a sale or through a permanent write-down.

[5] Financial Accounting Standards Board (FASB), Accounting Standards Codification (ASC) 330–10–35 Subsequent Measurement.

Evidence of accumulating losses may lead the auditor to conclude that management is intentionally delaying the recognition of such a loss.

Fictitious Investments Similar to the creation of other fictitious assets, fictitious investments can often be spotted by an absence of supporting documentation, missing brokerage statements, or investments that are unusual (gold bullion, for example) or held in remote locations or with obscure third parties. Among the steps an auditor who has a concern regarding the validity of investments might take are to confirm the existence of the investment by physical inspection or by confirmation with the issuer or custodian and to confirm any unsettled transactions with the broker-dealer. Beware of confirmations from custodians who are related parties. Auditors may also review the minutes of board of directors' meetings and the company's treasury policies to ensure that all investments were authorized by the board and that company policy was followed in the trading of and investment in securities. In addition, they may review internal controls to ensure that the duties of purchasing, recording, and custody are adequately segregated.

Manipulating the Value of Investments Companies can manipulate their financial statements by inflating the value of investments, misclassifying them, or failing to record unrealized declines in market value for those investments. ASC 820 "Fair Value Measurements and Disclosures" (August 2009) emphasizes the fair value hierarchy as a means to increase consistency and comparability in fair value measurements and related disclosures. The fair value hierarchy prioritizes the inputs to valuation techniques used to measure fair value into three broad levels. The fair value hierarchy gives the highest priority to quoted prices (Level 1) and the lowest priority to unobservable inputs (Level 3).

Specifically, Level 1 inputs are defined as quoted prices (unadjusted) in active markets for identical assets or liabilities that the reporting entity has the ability to access at the measurement date. Level 2 inputs are defined as inputs other than quoted prices included within Level 1 that are observable for the asset or liability, either directly or indirectly. Level 3 inputs are defined as unobservable inputs for the asset or liability. The level in the fair value hierarchy within which the fair value measurement in its entirety falls shall be determined based on the lowest level input that is significant to the fair value measurement in its entirety. Assessing the significance of a particular input to the fair value measurement in its entirety requires judgment, considering factors specific to the asset or liability.[6]

GAAP requires that debt securities and equity securities be classified as either trading, held to maturity, or available for sale.[7] Investments may be classified as held to maturity only if the holder has the positive intent and ability to hold those securities to maturity. Held-to-maturity securities are reported at amortized cost with no adjustment made for unrealized holdings gains or losses unless the value has declined below cost and is not expected to recover. In the latter instance, the security is written down to fair value, and a loss is recorded in earnings.[8] GAAP requires that

[6] FASB, ASC 820–10–35 "Fair Value Measurements and Disclosures," par. 35–55.
[7] FASB, ASC 320–10–25 "Classification of Investment Securities," par. 1.
[8] FASB, ASC 320–10–35 Subsequent Measurement, par. 1.

investments be classified as trading if they are bought and held principally for sale in the near term, that is, within hours or days. Investments in debt securities and equity securities that have readily determinable fair values and are not classified as trading or as held to maturity, are classified as available-for-sale securities.[9]

Trading and available-for-sale securities are reported at fair market value and must be adjusted periodically for unrealized gains and losses to bring them to fair market value. Unrealized gains or losses from trading securities are included in income for the period. Unrealized gains or losses from securities held as available for sale are reported as a component of other comprehensive income.[10]

In contrast, equity securities can be classified only as trading or available for sale. Unrealized gains or losses from changes in fair market value are reported in earnings for trading securities and as a component of other comprehensive income for securities held as available for sale.

When a security is transferred from one category of investment to another, it must be accounted for at fair value. Securities transferred from the trading category will already have had any unrealized holding gain or loss reflected in earnings. For securities transferred into the trading category, the unrealized holding gain or loss at the date of the transfer must be recognized in earnings immediately. For a debt security transferred into the available-for-sale category from the held-to-maturity category, the unrealized holding gain or loss at the date of the transfer must be reported in other comprehensive income. The unrealized holding gain or loss at the date of the transfer that results from securities' being transferred from available for sale to held to maturity is reported as a separate component of other comprehensive income and is amortized to interest income over the remaining life of the security.[11]

Generally, auditors looking into investments may consider asking management about company policies regarding the recording of unrealized gains or losses on trading and available-for-sale securities. The auditors may also ask accounting personnel whether they have been asked either to record held-to-maturity securities at anything but amortized cost, or to not record all unrealized gains and losses in available-for-sale and trading securities, or to postpone a write-down of a debt security.

Misclassification of Investments Companies can manipulate financial statements by intentionally misclassifying securities or transferring securities to a class that would trigger the recognition of gain or, conversely, postpone recognition of a loss. A company might, for example, misclassify a debt security as held to maturity to avoid recognizing a decline in value in the current period. Similarly, transferring a security from held to maturity to either trading or available for sale would permit the recognition of gains that had not previously been recognized. The treasury function commonly decides the classification at the time the security is acquired. Auditors may review any changes in classification for possible abuse.

---

[9] FASB, ASC 320–10–25 Classification of Investment Securities, par. 1.

[10] *Other comprehensive income* is generally defined as the change in equity of a business enterprise during a period from all transactions and events except those resulting from investments by owners and distributions to owners.

[11] FASB, ASC 320–10–35 Subsequent Measurement "Transfers of Securities Between Categories," par. 10.

Recording Unrealized Declines in Fair Market Value

Deciding whether to write down a security because of a permanent decline in value is highly subjective and ordinarily left to the discretion of management. Accepting a write-down results in a charge against net income. The auditor may consider whether management has inappropriately failed to record or has delayed the write-down of an impaired security for the purpose of inflating income.

Manipulating Cash Balances

As we have stated earlier, cash is the asset most often misappropriated. It can also be the subject of financial statement manipulation, however. There was a huge fraud that was allegedly perpetrated by senior management of a large company in Europe that involved various different fraud schemes including the overstatement of its cash and securities balances.

According to an SEC complaint, the Parmalat Finanziaria S.p.a. (Parmalat) group purportedly held 3.95 billion euros (approximately $4.9 billion at the time) worth of cash and marketable securities as of the end of 2002 in an account at the Bank of America in New York City, held by Parmalat's subsidiary Bonlat Financing Corporation (Bonlat). Bonlat was wholly owned by Parmalat and incorporated in the Cayman Islands. Bonlat's 2002 financial statements were certified by Bonlat's auditors based upon a false confirmation that Bonlat held these assets at the Bank of America. The accounts and assets allegedly did not exist and the purported confirmation had been forged. These nonexistent assets were reflected on Bonlat's 2002 books and records, in Parmalat's 2002 consolidated financial statements, and in its consolidated financial statements as of June 30, 2003.[12]

According to press reports, several confirmations were falsified over a period of time by Parmalat employees and submitted to auditors who relied on the information. An employee allegedly created a forged confirmation by scanning the bank's logo and a bank employee's signature, printing the document, copying and faxing it several times to conceal any imperfections, and ultimately faxing the final version to the auditors. The bank later reported that they had no record of the alleged account. The Parmalat fraud was allegedly perpetrated to cover up losses in certain businesses in addition to expenditures for nonbusiness purposes.

Detection of forged documentation can be difficult for an auditor or indeed a forensic accounting investigator. The auditor or investigator may wish to confirm material account balances directly with the bank or third party and not rely on faxed confirmations. In the Parmalat scandal, several fraud indicators were present that might suggest that additional audit procedures may be warranted:

- Dominant chief executive plus loyal chief financial officer
- Complex group structure that was not warranted by the operational needs of the business
- Increasingly frequent debt offerings despite apparent cash surpluses
- Multiple related-party transactions

[12] SEC Complaint Case No. 03 CV 10266 (PKC) (S.D. N.Y.) (December 29, 2003).

Recording Fictitious Fixed Assets

Similar to the concept of recording fictitious sales or receivables, companies can record fictitious assets to improve the balance sheet, thus also inflating earnings. Among the possible red flags associated with this scheme are:

- Fixed assets on the books and records that do not have an apparent relation to the business
- Lack of a subsidiary ledger to record additions and retirements
- Lack of adequate policies and procedures to determine whether property and equipment have been received and properly recorded
- Lack of procedures to account for fixed assets that may have been moved from one facility to another
- Existence of a secondhand storage facility for fixed assets that may still have useful life but for some reason are not being used
- Lack of adequate written policies and procedures concerning the recording, retirement, and disposition of fixed assets
- Subledgers that do not reconcile to the general ledger

If auditors find any of the foregoing, they may:

- Tour the client's facility to review fixed assets and select certain fixed assets from the fixed-asset listing—especially new, significant additions—to physically confirm that they exist. The assets' serial numbers may be inspected, if possible.
- Determine that retired assets are no longer included in financial statements.
- Review internal controls to ensure that written policies cover retirement procedures, which may include sequentially numbered retirement work orders, reasons for retirement, and all necessary approvals.

Depreciation and Amortization

An easy way to inflate the value of an asset and correspondingly reduce period expenses is to extend the asset's depreciable or amortizable life. Depreciation is another area in which management is given leeway to choose any method so long as that method allocates the costs to accounting periods over the useful life of the asset in a "rational and systematic manner."

Detection of such schemes begins with a review of depreciation policy. Most companies have written policies for depreciating assets, and the lack of a written policy heightens the potential for abuse. Similarly, recent changes to the depreciation policy may be scrutinized for both their purpose and the effect on assets.

Auditors who have suspicions may:

- Review the records of depreciable assets for unusually slow depreciation or lengthy amortization periods.
- Compare prior years' depreciation charges with the current year for reasonableness.
- Identify changes in policy that may affect the rate of depreciation and appear to boost earnings.

- Inquire into historical depreciation policies to determine the extent of their aggressiveness.
- Review a detailed list of fixed assets as well as the assigned lives of the assets—and then randomly select certain fixed assets and recalculate the net book value at reporting date based on the recorded life of the asset.

Hanging the Debit

As every accountant knows, for every credit there must be a debit. When companies spend money or incur costs, they recognize the event by posting a credit to cash, accounts payable, or accrued expenses. The offsetting debit will recognize that either an asset has been acquired or an expense has been incurred. A favorite tactic of financial statement fraudsters is to record expenses as assets—that is, to hang the debit up in the balance sheet. The WorldCom case is perhaps the starkest example of how a company can inflate earnings through improper capitalization of expenses. According to the Breeden Report, the company's internal audit department discovered that management had categorized as capital expenditures in 2001 billions of dollars that were, in fact, ordinary expenses paid to local telephone companies to complete calls. The scheme enabled WorldCom to turn a $662 million loss into a $2.4 billion profit. Experience has shown that certain categories of costs are the likely targets of such schemes.[13]

Software Development Costs

GAAP requires that companies treat as expenses those costs associated with developing software—up to the point of technological feasibility. Technological feasibility is established upon completion of a detail program design or, in its absence, completion of a working model. At that point, all software production costs must be capitalized and subsequently reported at the lower of unamortized cost or net realizable value.[14]

Whether technological feasibility has been reached is a subjective decision and thus subject to abuse. Arbitrarily determining technological feasibility, management can manipulate income by increasing or decreasing the amount capitalized or expensed. Auditors may consult with company engineers, programmers, and other technical personnel in reviewing management's assertions that technological feasibility has been achieved.

Research and Development Costs

On one hand, GAAP generally requires that R&D costs be expensed because of the uncertainty of the amount and timing of economic benefits to be gained from R&D. On the other hand, a company may capitalize materials, equipment, intangibles,

[13] Richard C. Breeden, *Restoring Trust,* Report to the Hon. Jed S. Rakoff, the United States District Court for the Southern District of New York on Corporate Governance for the Future of MCI, Inc. (August 2003).
[14] FASB, ASC 985–20–35 Subsequent Measurement "Net Realizable Value of Capitalized Software Costs," par. 4.

or facilities that have alternative future uses.[15] The U.S. Securities and Exchange Commission (SEC) has expressed particular concern about mergers in which the acquirers classify a large part of the acquisition price as in-process research and development, thus allowing the acquirer to expense the costs immediately.[16] This practice also involves the creation of liabilities for future operating expenses.

The SEC took action against Pinnacle Holdings, Inc.—arising from the latter's acquisition of certain assets from Motorola—after it found that Pinnacle had improperly established more than $24 million of liabilities that did not represent liabilities at the time of the acquisition.[17] The company entered into a settlement with the Commission as a result of the enforcement action.

Start-Up Costs

As with R&D, GAAP requires all start-up costs to be expensed in the year incurred.[18] It is not uncommon for companies to label start-up activities as other costs for the purpose of capitalizing them.

Interest Costs

One potential scheme in this area involves a company's continuing to capitalize interest after construction has been completed. Statement of Financial Accounting Standards (SFAS) 34, *Capitalization of Interest Costs*,[19] requires the capitalization of interest costs incurred during the acquisition and construction of an asset. The interest cost capitalized is added to the cost of acquiring the asset and then amortized over the useful life of the asset. The total interest cost capitalized in a period may not exceed the interest cost incurred during that period. Capitalization is no longer allowed when the cost of the asset exceeds its net realizable value.

Advertising Costs

In SOP 93–7, *Reporting on Advertising Costs*,[20] the American Institute of Certified Public Accountants provides that all advertising expenses must be expensed as incurred unless there is persuasive historical evidence that allows the entity to make a reliable estimate of future revenue to be obtained as a result of the advertising. In that case, the expenditures may be capitalized.

---

[15] FASB, ASC 730–10–25 Recognition "Elements of Costs to Be Identified with Research and Development Activities," par. 2.
[16] Arthur Levitt, "The 'Numbers Game' " (Speech, New York University Center for Law and Business, September 28, 1998), www.sec.gov/news/speech/speecharchive/1998/spch220.txt.
[17] See *In the Matter of Pinnacle Holdings, Inc.*, *Securities Exchange Act of 1934* (SEA) Rel. No. 45135; *Accounting and Auditing Enforcement* (AAE) Rel. No. 1476 (December 6, 2001).
[18] American Institute of Certified Public Accountants, Accounting Standards Executing Committee (AcSEC), Statement of Position (SOP) No. 98–5, *Reporting on the Costs of Start-Up Activities* (April 1998).
[19] FASB, ASC 835–20–25 Recognition "The Capitalization Period," par. 2–6.
[20] Issued December 29, 1993, and amended by SOP 00–2, June 2000.

In 2000, the SEC charged America Online (AOL) with incorrectly amortizing for fiscal years 1995 and 1996 the subscriber acquisition costs associated with the manufacture and distribution of computer discs containing AOL software. The SEC asserted that the volatile, unstable nature of Internet businesses had made it impossible for AOL to predict reliably its future net revenues. Thus, the SEC concluded, the subscriber costs were more like advertising costs and required expensing in accordance with SOP 93–7. According to the SEC, AOL had reported profits for six of the eight quarters in 1995 and 1996 instead of the losses it would have reported had these costs been expensed. The costs improperly capitalized amounted to approximately $385 million by September 30, 1996, when AOL decided to write them off. In November 2004, Time Warner proposed a settlement to the SEC regarding its investigation of AOL's accounting for these costs.[21] According to the SEC, in March 2005, Time Warner agreed to a $300 million penalty, an antifraud injunction, and an order to comply with a prior cease-and-desist order, and Time Warner would restate its financial results to reduce its reported online advertising revenues by approximately $500 million (in addition to the $190 million already restated) for the fourth quarter of 2000 through 2002 and to properly reflect the consolidation of AOL Europe in the company's 2000 and 2001 financial statements. Time Warner also engaged an independent examiner to determine whether the company's historical accounting for certain transactions was in conformity with Generally Accepted Accounting Principles (GAAP).

UNDERSTATEMENT OF LIABILITIES AND EXPENSES

An understatement of liabilities and expenses is the mirror image of an overstatement of assets, and auditors can use various analytical indicators to search for such schemes. Among them are:

- An increasing current ratio (current assets divided by current liabilities) or quick ratio (cash plus marketable securities plus net receivables divided by current liabilities) from one period to the next
- Unexpected improvements in gross margins from one period to the next
- Change in inventory with no simultaneous increase in accounts payable or accrued expenses between periods
- A percentage of change in the accrued expense account that shows revenue to be increasing faster than accrued expenses

The auditor may also ask accounting personnel whether they have ever been asked to postpone expenses until a subsequent period. The auditor may also:

- Review the expense ledger and perform a cutoff test to ensure that expenses have been recorded in the proper period and not postponed until a subsequent period.
- Review prior years' expenses and liabilities and look for unusual trends.

[21] James Bandler and Michael Schroeder, "Time Warner, SEC Are Moving to Settle AOL Accounting Probe," *Wall Street Journal,* November 24, 2004.

- Perform current or quick-ratio analysis, which may indicate the concealment of liabilities.
- Examine account detail, looking for unusual debits to liabilities that would have the effect of reclassifying an expense to the balance sheet and also of improving the current ratio. (Certain levels of current ratio may be required for debt covenant compliance.)
- Consider data mining to identify significant payments for further review and then determine whether the payment may have been capitalized.
- Review internal controls regarding recognition of expenses in the proper period.
- Review capitalized expenditures to determine whether they are more appropriately classified as expenses.

BACKDATING SHARE OPTIONS

As a supplement to salary, companies frequently offer employees stock options, which grant the recipient the privilege to purchase a share of the company's stock at a future date for a specific price, called the strike price. A strike price is the value of a share at a particular date. Generally, the strike price is set at the price of the underlying stock on the day the option is granted; therefore the option becomes valuable only with future increases in the stock price.

In this way, companies grant stock options as an incentive for employees to boost company performance and thus raise the stock price. However, the practice of backdating stock options gives the employee a chance to profit by purchasing stock at past low prices, providing an immediate payoff. Backdating stock options occurs when a company alters the date of the grant to a time when the stock was trading at a lower price in the interest of making the option instantly valuable and further increasing the employee's gain if the stock price continues to rise.[22]

For example, on June 1, 2006, Company XYZ grants its CEO a stock option that provides the executive the right to purchase 100 shares of XYZ stock on January 1, 2007, for the strike price. Per its usual policy, the strike price is set at the price of the company stock on the date of the option grant. On June 1, 2006 (the grant date), XYZ stock was trading at $40 per share. Therefore, if the stock price increases to $45 per share by January 1, 2007, the CEO could exercise the option and purchase the shares for $40 per share, then sell them immediately on the market for $45 per share, resulting in a gain of $5 per share. However, the company has recently experienced a dramatic increase in its share price. On May 24, 2006, the stock was trading for $15 per share. To provide the CEO with an opportunity to exploit this increase in share price, even though it has already occurred, the company chooses to date the stock options as if they were granted on May 24, 2006. Because the strike price is set at the price of the stock on the option grant date, the strike price is effectively changed to $15 per share. As a result, the CEO now has the option to buy 100 shares of XYZ stock on January 1, 2007, for $15 per share. Thus, the CEO has immediately gained $25 per share (the difference between the stock price on the actual grant date of June 1 and the stated grant date of May 24) based solely on the manipulation of the grant date used.

---

[22] Association of Certified Fraud Examiners, *2008 Fraud Examiners Manual,* Section 1.1544.

Suggested audit procedures include:

- Review the control procedures relating to stock option grants.
- Obtain a list of all stock option grants for officers and directors of the company as reported in public filings. Ensure the dates of the grants per the public filing agree with those approved by the board of directors.
- Review the company's stock performance for a period of time before and after the grants and look for peaks and valleys.
- If the stock option grants coincide with valleys in the chart, a potential for backdating may exist.
- Review stock option grants before and after favorable and unfavorable press releases and public filings.
- Review the stock option policies and procedures enforced by the Compensation Committee.

OFF-BALANCE-SHEET TRANSACTIONS

A legacy of Enron's collapse has been to make the term *off-balance-sheet transactions* part of everyday business vocabulary. In off-balance-sheet transactions, a company retains the benefits of assets in a corporate vehicle not consolidated for financial accounting purposes. Such investments can typically appear in the asset section of the balance sheet as a single net line item, titled *Investment in Affiliate,* or *Retained Interest in Securitization,* or some other such term. Off-balance-sheet transactions enable the company to avoid showing the individual asset of the off-balance-sheet vehicle in the balance sheet and, more important, the associated debt used for acquiring its assets. In other words, the company executing the transaction reports only its proportion of the *net* assets of the off-balance-sheet vehicle as an asset rather than the *gross* assets of the vehicle, including the vehicle's total debt and outside interests held by other parties. While this form of reporting technically would not change the *net* equity of the company executing the transaction, the consolidated balance sheet would show greater total assets and greater total debt. Thus, in executing an off-balance-sheet transaction, the company looks more financially attractive. Balance-sheet-dependent financial ratios are also affected. Debt-to-equity ratios will be higher, for example, and thus less favorable, under consolidation treatment than under nonconsolidation.

Historically, off-balance-sheet treatment has been used:

- For securitization transactions, in which financial assets such as receivables are sold to an off-balance-sheet vehicle, while the seller retains a subordinated interest in that entity.
- For leasing transactions in which long-lived assets are acquired by an off-balance-sheet entity and the use of the assets is then conveyed to a third party through an operating lease.
- In noncontrolling investments, in which assets or businesses are held by an entity that does not convey control back to the investors: One simple example is a jointly controlled joint venture; the assets and debt of that venture remain off balance sheet for at least one of the partners or investors involved.

The collapse of Lehman Brothers in September 2008 has been attributed to numerous factors, one of them being the use of an accounting device (known within Lehman as *Repo 105*) to manage its balance sheet, by temporarily removing approximately $50 billion of assets from the balance sheet at the end of the first and second quarters of 2008. The March 11, 2010, report issued by Examiner Anton R. Valukas stated that according to Lehman's global financial controller, "the only purpose or motive for Repo 105 transactions was reduction in the balance sheet" and that "there was no substance to the transactions." The report also states that in addition to balance sheet manipulation, Lehman's failure can be attributed to serious business judgment errors made by Lehman executives, to the investment bank's flawed business model (which rewarded excessive risk taking and leverage), and to government agencies, who by their own admission might have better anticipated or mitigated the outcome.

TWO BASIC ACCOUNTING MODELS

Before Enron's collapse, accounting rules relied on two basic models to determine whether consolidation treatment was proper. The first focused on voting control and required consolidation if one entity controlled another. This model was relied on heavily in situations in which the subject of the analysis was a business rather than a pool of assets and debt.

The second model was the special-purpose-entity (SPE) model. Factors typically indicating that a vehicle is an SPE are limited powers in the vehicle's charter or the housing of assets—not a business—for which there was a limited purpose and about which few decisions needed to be made. The potential for abuse generally occurred through:

- Manipulation in the determination of whether to apply the voting control or the SPE model to a transaction
- Manipulation in the application of the correct accounting model
- Aggressive use of the wrong accounting model

After Enron's collapse, the Financial Accounting Standards Board expanded on the accounting guidance that governs when a company may include in its own financial statements the assets and liabilities of another entity. Financial Interpretation No. (FIN) 46, *Consolidation of Variable Interest Entities,* as amended by Accounting Standards Update No. 2009–17, applies consolidation requirements to applicable entities created after January 31, 2003. The technical rules are complex but can be summarized briefly. The underlying principle is that if a business enterprise has the majority financial interest in an entity (defined as a *variable interest entity,* or VIE), then the assets, liabilities, and results of the activities of the VIE should be included in consolidated financial statements with those of the business enterprise. A company that consolidates a VIE is called the primary beneficiary of that entity.

In general, a VIE is a corporation, partnership, trust, or any other legal structure used for business purposes that does not have sufficient equity investment at risk to permit it to finance its activities without additional subordinated financial support. The interpretation is also applicable to an entity whose equity holders have neither

the direct nor indirect right to make decisions about its activities through voting rights or similar rights, nor the obligation to absorb the expected losses of the entity if they occur, nor the right to receive the expected residual returns of the entity. A VIE often holds financial assets—including loans or receivables, real estate, or other property.

FIN 46 emphasized a risk-and-reward model of consolidation and contained a scope test that served to determine whether an off-balance-sheet entity is a VIE and thus whether the provisions of FIN 46 govern and require consolidation of the off-balance-sheet entity. An amendment to FIN 46 was published on December 22, 2009 (Accounting Standards Update No. 2009–17). The amendment replaced the quantitative-based risks and rewards calculation for determining which reporting entity, if any, has a controlling financial interest in a variable interest entity. The new approach focuses on identifying which reporting entity has the power to direct the activities of a variable interest entity that most significantly affect the entity's economic performance and the obligation to absorb losses of the entity or the right to receive benefits from the entity. This approach is expected to be primarily qualitative and likely more effective for identifying which reporting entity has a controlling financial interest in a variable interest entity.

Obviously, hiding or disguising information from the auditor or the investing public is the easiest way for a company to keep assets and liabilities off its books or to inflate income. Management might also manipulate the estimate of expected losses in its cash flow projections so it can obtain off-balance-sheet treatment. Manipulation can take many forms, such as failing to recognize impairments that would decrease expected cash flows. Auditors will need to consider the potential of these schemes on a case-by-case basis.

COOKIE JAR RESERVES

A variation on these overstatement and understatement schemes occurs when companies overstate the amount of provisions to cover the expected costs of liabilities such as taxes, litigation, bad debts, job cuts, and acquisitions. This may be done in years when a company is extremely profitable, so that it can afford to incur larger expenses. These so-called cookie jar reserves are then tucked away for management to reach into and reverse in future years when profits may slip and a boost to earnings is judged necessary.

Intentional underestimation of loss contingencies and loss accruals is another subjective area ripe for abuse. This can affect items such as allowance for doubtful accounts, litigation reserves, inventory reserves or lower-of-cost-or-market write-downs, warranty reserves, and impairments of long-lived assets.

Company managers estimate reserves, and the outside auditor judges whether the reserves are reasonable. Because there are no clear accounting guidelines and judgment is required, it can be difficult for auditors and regulators to challenge company estimates. This creates the potential for abuse.

Be mindful of account descriptions. A title such as *Miscellaneous Provisions* may be an indicator of a cookie jar reserve account. In a recent investigation, the external auditor asked the internal auditor to identify which account the company used when it needed to make the numbers. Without hesitation, the internal auditor cited the

number of an account named Miscellaneous Provisions. Through account analysis and collaboration with company employees, the external auditor determined that more than $7 million was in this account for use on a rainy day. The explanation provided by the company was that it had already met its goals of paying bonuses for the end of the period, and this account represented a reserve if needed for future periods.

In June 2004, the SEC charged Symbol Technologies, Inc. with a variety of offenses. The commission's complaint alleged that from 1998 through 2002, Symbol and certain former executives had engaged in numerous fraudulent accounting practices and other misconduct that had a cumulative net impact of over $230 million on Symbol's reported revenue and over $530 million on its pretax earnings.[23]

The SEC complaint alleged that executives engaged in a fraudulent scheme to inflate revenue, earnings, and other measures of financial performance for the purpose of creating the false appearance that Symbol had met or exceeded its financial projections. Among other fraudulent accounting practices, the former executives were charged with the fabrication and misuse of restructuring and nonrestructuring charges to artificially reduce operating expenses, create cookie jar reserves, and manage earnings. According to the SEC, the release of the cookie jar reserves into earnings improperly boosted earnings and was not disclosed to the public at the time.[24]

IMPROPER AND INADEQUATE DISCLOSURES

To this point in the chapter, we have focused on financial statement fraud involving numbers, but a company can also misrepresent its financial condition through misstatements and omissions of the facts and circumstances behind the numbers. These might include descriptions of the company or its products in news reports, interviews, and annual reports; on web sites; and in management discussions and other nonfinancial-statement sections of annual reports, Forms 10-K, Forms 10-Q, other documents, other reports, and footnotes to the financial statements.

In these instances, management has perpetrated a fraud by not providing sufficient information to make an informed decision regarding the financial position of the company.

The Sarbanes-Oxley Act of 2002[25] attempts to correct many of the shortcomings of nonfinancial disclosures. Sarbanes-Oxley requires that CEOs and chief financial officers (CFOs) acknowledge their duty to establish and maintain "disclosure controls and procedures" (DC&P) and to confirm their effectiveness. *DC&P* is a new term that expands traditional notions of internal controls to include both financial and nonfinancial information. DC&P encompasses all of the information in the company's public filings, including market share, information on the competitive environment, the regulatory environment, business goals, objectives and strategy, governance matters, planned acquisitions, customers, supply chain, and contracts.

---

[23] SEC Litigation Rel. No. 18734 (June 3, 2004).
[24] Id.
[25] 17 CFR Parts 228, 229, 232, 240, 249, 270, and 274 (August 29, 2002), § 302.17.

The law also requires prompt disclosure in plain English of all material changes in financial condition and of other significant company news, as well as disclosure of off-balance-sheet transactions as defined under the statute.[26] Realistically speaking, Sarbanes-Oxley is likely to lead to an array of new fraud schemes, as unscrupulous companies and individuals seek to circumvent the disclosure requirements and other reforms. A recent example of disclosure fraud was provided by the controversial circumstances surrounding Bank of America Corporation's acquisition of Merrill Lynch and Company. In February 2010, the SEC filed a motion seeking court approval of a proposed settlement whereby Bank of America will pay $150 million and strengthen its corporate governance and disclosure practices to settle SEC charges that the company failed to properly disclose employee bonuses and financial losses at Merrill Lynch before shareholders approved the merger of the companies in December 2008.[27]

Some commentators have also asserted that improvements to internal controls prompted by Sarbanes-Oxley have reduced the incidence of financial statement fraud. It is worth remembering that fraudsters are infinitely creative and no practical system of internal controls will completely prevent the occurrence of fraud and misconduct.

MATERIALITY

No discussion of financial statement fraud is complete without taking up the issue of materiality. Companies—and sometimes auditors—have dismissed possible mistakes by concluding that they are not material to the financial statements. The issue of materiality draws on both legal and accounting principles. Guidance can be found from the U.S. Supreme Court, the SEC, the FASB, and academic literature. The Supreme Court has defined something as material if "there is substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[28] The SEC, in Regulation S-X, defines *material items* as "those matters about which an average prudent investor ought reasonably to be informed" before purchasing the registered security.[29] The FASB has defined *materiality* to be "the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying

[26] The statute requires companies to "disclose all material off-balance sheet transactions, arrangements, obligations (including contingent obligations), and other relationships of the issuer with unconsolidated entities or other persons that may have a material current or future effect on the issuer's financial condition, results of operations, liquidity, capital expenditures, capital resources or significant components of revenues or expenses."
[27] SEC Litigation Release No. 21407/February 4, 2010.
[28] *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976).
[29] 17 CFR Part 210, Reg. § 210.1–02. Rule 1–02: "... (o) Material. The term material, when used to qualify a requirement for the furnishing of information as to any subject, limits the information required to those matters about which an average prudent investor ought reasonably to be informed."

on the information would have been changed or influenced by the omission or misstatement."[30]

Over time, companies and auditors had developed certain rules of thumb to assist them in determining when a matter might be material. One is that a misstatement or omission that represents less than 5 percent of some factor (such as net income or net assets) is not material. The SEC sought to settle the issue of materiality and remedy the potential for earnings management abuse with the 1999 release of Staff Accounting Bulletin (SAB) No. 99, *Materiality*.[31] SAB 99 provides guidance for preparers and auditors on evaluating the materiality of misstatements in the financial reporting and auditing process by summarizing and analyzing GAAP and federal securities laws and offering examples of what is and is not acceptable.

While the SEC does not object to the use of the 5 percent threshold for a preliminary assessment of materiality, it emphasizes that the final determination must be based on an analysis that considers qualitative factors rather than relying exclusively on a quantitative benchmark. SAB 99 notes specifically that certain qualitative factors can cause even quantitatively small misstatements to become material. It suggests that auditors must determine whether the misstatements:

- Arise from imprecise estimates
- Mask changes in earnings trends
- Cause financial statements to meet analysts' expectations
- Would change a loss to income or income to a loss
- Affect compliance with regulations or contracts
- Affect management compensation
- Arise from illegal acts

Auditors question the facts and circumstances of suspicious transactions. Auditors may, for example, make document requests that give the client information about materiality and scope, such as "provide documentation for all transactions in account XX over $5,000." As a result of this communication, a fraudster on staff may decide to embezzle funds at transaction amounts of less than $5,000. While an individual transaction of less than $5,000 may fall below the auditor's scope, the amount of the embezzlement may be material as it relates to the financial statements. When there is any suspicion of this kind, the auditor may consider consultation with a forensic accounting investigator, who can offer assistance and guidance in the selection of additional procedures and in the performance of those procedures.

DISBURSEMENT SCHEMES

A fraudulent disbursement is a payment of an entity's funds for a purpose that is not performed to benefit the entity. That is, the payment satisfies no obligation and serves no need of the entity. In contrast to schemes that steal cash at point of

[30] Financial Accounting Standards Board, Statement of Financial Accounting Concepts (SFAC) No. 2 (1980), 10.
[31] Issued August 1999.

entry, fraudulent disbursement schemes involve theft of funds already entered into the books and records.

The audit objective with respect to cash is to verify the actual cash balance. As the actual cash balance gets reduced by fraudulent disbursements, typical audit procedures related to cash will detect only that the cash has been used and will not detect that the cash has been used inappropriately. Bank control procedures—such as positive pay, dual-signature requirements, and rejection of items with secondary endorsements—are not foolproof barriers to the creative fraudster. Positive pay systems, for example, do not prevent payments to a bogus vendor the fraudster has set up—payments the fraudster will convert.

Fraudulent disbursements, in order of frequency, are accomplished primarily through invoice schemes, vendor kickbacks, check tampering, expense reimbursement schemes, and payroll schemes. Occasionally, such schemes are used in combination. The following is a discussion of detection techniques related to these schemes.

INVOICE SCHEMES

In invoice schemes, which account for almost half of fraudulent disbursement schemes, fraudulent invoices are submitted to the company for payment. The invoices can be submitted either by a third party or by an employee. In many of these schemes, an employee creates a shell company and then submits fictitious invoices from the shell company to his employer for payment. The invoice is often for consulting or other services, since there is no way to physically verify receipt of the invoiced item—as there would be for inventory or supplies. The employee perpetrator must have the ability to add vendors to the approved-vendor list, to approve vendor invoices, or to obtain the approval of a vendor invoice through altered or fictitious documents or through a supervisor who performs only a cursory review of documents requiring approval.

In one case, a public relations and investor relations officer used a false-invoice scheme to take from his employer $1 million per year for 10 years. He did this by having business associates of his wife fax him "invoices" for public relations services in Europe. As one of the five top officers in the company, he would approve the invoices and issue payment instructions through the company's regular disbursement process. Because of his seniority, no one ever questioned the fax copy of the invoice or the meager description of services. Since he was careful to budget the amount he would steal each year, he was never over budget and he escaped detection by budgetary controls. In fact, the payments were going to a series of antiques dealers throughout Europe to pay for inventory purchases by his wife's antiques shop. The court reduced his jail term to only a few years because of the substantial restitution he made from selling off the antiques.

While less common, another invoice scheme is one that also involves personal purchases with company funds. In cases of this kind, the invoices are legitimate in that they're from real vendors that actually provide goods and services on a recurring basis. The goods and services, however, are not provided for the benefit of the company but for the benefit of the employee.

The primary detection methods for invoice schemes are statistical sampling, data mining, and analytical procedures. Samples of source documents supporting

purchases—usually the voucher file—may be selected and examined for irregularities. Possible red flags might include:

- No address given for the vendor or no physical address shown: only a post office box
- No invoice number
- Invoice numbers from the vendor that are sequential and with no gaps, thereby implying that the vendor issued invoices to no one other than the victim company
- No reference to a purchase order number, an order date, or the name of the individual placing the order
- No engagement letter or other documentation reflecting authorization for services
- No detail given about the goods or services provided
- No information available regarding a contact person or phone number for the vendor
- Numerous purchases at approximately the same dollar amount, especially if that amount is just below a particular authority approval level
- No indication of payment terms—or payment terms not in line with industry norms

For files containing irregularities, it may be appropriate to:

- Call listed phone numbers to see whether anyone answers the phone or whether an answering service responds.
- Check for directory assistance listings.
- Check for listings with the secretary of state and obtain information about the incorporators.
- Confirm the existence of the physical address.
- Check for credit reports with Dun and Bradstreet or a similar credit reporting agency.
- Perform related procedures, such as data mining along the following lines:
  - Vendors with only a post office box for an address
  - Identical addresses in vendor files and in employee files
  - Vendors with similar names
  - Transactions for amounts invoiced just below an approval level
  - Recently added data

Analytical procedures may consist of performing trend analyses on various expense line items to identify any unexpected increases in spending categories, as well as trend analyses on vendors. Manual journal entries to expenses may be examined.

One scheme involving vendors with similar names was accomplished by an ad agency account executive whose agency processed about $500 million in media purchases and commercial production payments for a major consumer goods company. He opened a bank account in the name of William Morris, mimicking the name of the well-known talent agency, William Morris Agency. The invoices supporting the payments were typed by his secretary and always returned to him because they required prompt processing so as not to delay the production schedule. The fraudulent disbursements were hidden in the large volume of payments processed for the

client—until the client's account developed a permanent out-of-balance condition of several million dollars. Internal auditors were assigned to investigate. The scheme was discovered one day when the head of internal audit, on the point of entering the executive's office, was asked in the hallway by the CFO how the analysis of the William Morris invoices was going. The fraudster's secretary, overhearing the question, helpfully interjected that she could no doubt answer any questions because, after all, she had prepared them!

Another invoice scheme was perpetrated by employees of a retail operation. The employees at a store location submitted false invoices to corporate headquarters, generally for maintenance work performed on the store. The employees persuaded the headquarters office to send the checks back to the employees rather than directly to the vendors. The employees then deposited into the local bank account for the store the checks written to the vendors. The same amount of cash was then stolen. Both of these schemes might have been prevented if checks had been sent directly to vendors instead of being returned to the requesters.

A good deterrence technique is to continually purge inactive vendors. The easiest way to set up a vendor-based scheme is to take an inactive vendor from the approved listing and change the address to one controlled by the perpetrator. It is then easy enough to submit bogus invoices from this "approved vendor." Approvers may recognize a vendor they have not seen in a while, but they will almost never recognize the vendor's address. Thus, a change of address rarely draws the attention of those responsible for approving such payments. A former controller of a well-known hotel misappropriated more than $15 million in cash by setting up a dummy corporation and issuing phony invoices for services never rendered. The controller was able to get away with the scheme for more than six years because he maintained sole control over the hotel bank account and was able to submit phony invoices and issue checks or wire funds to the dummy corporation he controlled.

A variation on the invoice scheme is for employees with responsibility or oversight over the procurement function to make an arrangement with vendors whereby an organization will purchase all or most of a particular product or service from a preferred vendor. The procurement will usually be for valid products or services. The fraud will generally be effected through a small increase in the price. In return for this preference, the vendor may be allowed to increase the normal price of the goods or services by a marginal amount—usually designed to be difficult to notice in the context of the overall cost of the service or product. This surcharge, or mark-up, is then used by the vendor to finance payments to the buyer, procurement manager, or senior executive personally—sometimes called a *kickback, commission,* or *facilitating fee.*

In the case of this type of vendor kickbacks, it can be quite difficult for the auditor or forensic accounting investigator to discover the fraud scheme. There will, by definition, be collusion, so the auditor should inquire into the procurement process. Questions may include whether the organization requires competitive bidding for procurement contracts in excess of specified limits or periods of time. An indication of potential fraud may be provided if one particular vendor continues to be used despite complaints or indications of higher than necessary prices being charged by a long-standing vendor. Another red flag may be raised if one particular buyer, manager, or senior executive maintains the sole contact and relationship with any significant vendor.

CHECK TAMPERING

In check-tampering schemes, the perpetrator takes physical control of a check and makes it payable either to himself, to a shell corporation he controls, to an accomplice, or to cash. The scheme can include obtaining blank check stock or taking checks after they've been made payable to other parties and altering them so that they're payable to or for the benefit of the fraudster. In the case of preparing a check from blank check stock, the fraudster has to forge a signature or obtain a signature from a supervisor who performs only a cursory review of documents presented for signature. It is less common for the perpetrator to be the person with signature authority for the bank account. Altering checks that have already been prepared and signed generally occurs before the check is delivered to the intended recipient. It may also occur with returned checks—that is, checks returned due to undeliverable addresses or because there was an error in the check.

In one such scheme, the perpetrator intentionally double-paid vendors, then called the vendors and asked them to return the duplicate payment. Upon return of the check, the fraudster would alter it to be payable for his benefit. In a similar scheme, the controller of a lumber company wrote two checks for every tax payment. He added his own Social Security number to one of them before sending both of them to the U.S. Internal Revenue Service and would recover the money by claiming a tax refund on the one that showed his ID. He was detected by an audit inquiry directed to his accounting clerk as to why two checks to the same party on the same date would be necessary. When she replied that she had no idea but had always thought it odd, closer examination ensued and the scheme unraveled. These instances highlight the reasons to deface invoices so that they may not be used again; to reinforce a policy of paying only from original invoices, not copies; and to adequately segregate duties.

Check-tampering schemes may be difficult to detect through analytical procedures or data mining. Generally, the books and records reflect the intended and legitimate cash outflow. Complaints of nonpayment from suppliers whose payments were diverted by the fraudster are obvious red flags. Yet to detect check tampering, there is no substitute for visual inspection of the relevant documents:

- In the book balance for cash, be alert to voided or missing checks.
- Examine bank statements to make sure that voided checks did not clear the bank.
- In reviewing bank statements, carefully review the presented checks for possible alterations, forgeries, inappropriate payments, or other anomalies.
- Do not assume that a check with two signatures is unlikely to be part of a fraud scheme. It is not uncommon for both parties signing a dual-signature check to assume that the other party has carefully examined the veracity of the payment and underlying documentation, and, as a result, they each sign without review.
- Bank reconciliations may also be examined and all reconciling items analyzed.
- It may also be appropriate to request cutoff statements from the bank and perform an independent reconciliation as of that date.

One check-tampering scheme involving a private company was perpetrated through a variety of methods. The perpetrator, a financial officer of the company, had signing authority up to a maximum dollar limit and simply wrote checks for his benefit up to that limit. He also forged signatures on checks written for his benefit and altered the payee on checks with authorized signatures. Also, the perpetrator set up a bank account in the name of the company, on which he was the only signatory. He could then deposit company checks into this account. Unwinding this fraud took a detailed manual review of all checks and supporting documents. Frauds such as these can drain millions from a company and go undetected for years, if not forever—or until the company files for bankruptcy.

EXPENSE REIMBURSEMENT SCHEMES

Expense reimbursement schemes may seem like small change when compared with millions of dollars in fraudulently overstated inventory. Our experience is that if an employee is submitting false expenses, that scheme may be a potential red flag signaling other areas that may be subject to abuse. The same process applies for travel and expense reports as it does for purchase cards. Typically, purchase cards are used for smaller-dollar items; fraud may occur, however, when no one examines the details of statements from purchasers.

When suspicions of false expenses arise, consider the following approaches:

- Select employees by focusing on those with high-dollar reimbursements. The 80–20 rule may apply here: 20 percent of the employees may account for 80 percent of the travel and related reimbursements.
- Rather than randomly selecting a few expense reports for one individual over the course of a year, consider reviewing a span of expense reports consecutively. In the course of examining a span of expense reports, you may consider exporting the expense detail to a computerized tool for sorting. Using this technique is also helpful when examining a group of employees. Doing so will enable you to identify:
  - Duplicate amounts: Is the same amount reimbursed more than once? Is it possible to submit an airline itinerary for reimbursement on one report, and then two weeks later submit the boarding pass for the same itinerary, and two weeks after that submit the proof of payment from the credit card statement? If you randomly selected expense reports over the course of a year, you would miss the duplicate submissions.
  - Pay attention to currency exchange. Does it make sense that someone traveling to Mexico would submit a restaurant receipt in U.S. dollars? The answer is no.
  - Do people in the company normally entertain on weekends? Sort and identify weekend travel and ask whether the pattern of entertainment makes sense.
- Compare hotel bills across the selection. In one investigation, a forensic accounting team noticed hotel bills that were generic and similar. Upon closer inspection, the local telephone number proved to be the same on a hotel receipt in Washington state as for a hotel in Washington D.C. The fraudster had created

a hotel template and fabricated complete phony trips. In addition to the hotel phone bills, the fraudster booked airline tickets, submitted the itineraries, and later credited the airline ticket. When in doubt, call the hotel. You may discover that room 1304 does not exist at that location.

- Do the trips make sense? Is a salesperson traveling 800 miles while submitting meal charges for less than $25? Often, items of less than $25 do not require receipts. A salesperson can submit mileage and claim the remaining expenses as small cash items when the trip did not in fact occur.
- Are there tear-off receipts included in the documentation? If so, examine the receipts for consecutive numbering. The fraudster may have a pack of receipts, purchased from an office supply store, which he uses to document false expenses. Also, consider the country in which the expenses were incurred. In some countries, where cash is still widely used for all types of expenses, receipts are not as detailed, or itemized, and indeed may be from a completely different establishment from that claimed by the employee. In these circumstances, local review of expense reports and checking of vendors may be worthwhile.
- Are expenses submitted with the top torn off, so that the name of the establishment is not on the receipt? Ask to see the credit card statement for the payee. If the telephone number still appears on the receipt, call to get the name of the establishment. One fraudster submitted many receipts with the establishments' names torn off; however, the telephone numbers remained. Rather than for a hotel or a meal, the purchases proved to be for shoes and jewelry.
- Does the company reimburse credit card expenses without first examining and approving the detail? If so, take a closer look at the details of credit card purchases. One executive we investigated used the company credit card to purchase two bouquets of flowers weekly, one for the reception area of the offices and the other for his wife. While hardly material to the business, it was a red flag relating to the executive's integrity.
- Are gifts for clients or expenses paid to clients appearing on the expense reports? Maintain a watchful eye for potential Foreign Corrupt Practices Act (FCPA) violations, discussed in Chapter 26. In some instances, investigation has shown that an employee will pay a gift or bribe, such as digital cameras or airline tickets, through the expense report.

PAYROLL SCHEMES

Payroll schemes represent the payment of wages or other forms of compensation in excess of that earned by the employee. This is most often accomplished through the use of phantom employees and the falsification of time cards. Analytical review of and reasonableness tests related to payroll expense could reveal irregularities. Data mining, an effective detection technique for payroll schemes, can include data interrogation queries to identify:

- Employees who have no payroll deductions to be distributed to taxing authorities: Deducting taxes for bogus employees causes reconciling items to appear in Form 941.

- Employees without Social Security numbers—and to possibly take the step of verifying the accuracy of reported Social Security numbers as a way of identifying ones that may be bogus.
- Common data between different employees, including addresses and electronic deposit information: One of them may be bogus.
- Matching of payroll lists to employee lists maintained by the human resources department.
- Names appearing on payroll records after their termination date.

FRAUD IN AN ECONOMIC DOWNTURN

The impact of the credit crunch and the global economic slowdown is challenging even our most robust institutions. Those charged with the governance of some of the largest private sector companies have had to focus on short-term measures to address the risk of corporate failure. Leaders of public sector institutions must confront challenges around guarding against fraud, corruption, waste, and abuse in implementing multitrillion-dollar stimulus programs and maintaining and improving service provision when the resources necessary to deliver services may not be made available. The dilemma public and private organizations face is how best to manage recovery in the short term, while not losing sight of the need to maximize shareholder value and to maintain and develop services over the medium and long term.

As the economy is exposed to severe pressure, both in the United States and globally, new threats emerge. The recent collapse of certain investment companies illustrates how frauds, previously undetected, emerge from the shadows. As Warren Buffett famously stated: "Only when the tide goes out do you discover who's been swimming naked."[32] The Bernard Madoff Ponzi scheme is a great example of this and is discussed in detail in Chapter 24.

Possibly the only positive aspect of the credit crunch is that, as providers of finance retrench and see return of loan finance or investment capital, fraudulent borrowing or fraudulent investment management is revealed, thereby capping the losses that have occurred.

When economic survival is threatened (either for the organization or for the individual) the line separating acceptable and unacceptable behavior can, for some, become blurred. Also, fraud and other economic crimes have become a focus of criminal activity over the past several years; criminal organizations that profit from fraud view the current economic conditions as an opportunity, not a threat.[33]

UNAUTHORIZED TRADING

Rogue trading is the term used to describe unauthorized trading activities conducted by traders in the name of their employers. On any given day, it is possible for traders

[32] Warren Buffett, (n.d.), BrainyQuote.com, www.brainyquote.com/quotes/quotes/w/warrenbuff383933.html.
[33] Jonny Frank, *Fraud in a Downturn,* May 2009.

to operate outside of the established rules of an institution. Rogue trading is often exposed when markets decline and the value of the unauthorized positions drops, requiring the rogue trader to come up with additional sources of financing to cover the losses.

For example, an employee of Société Générale (France's second-largest bank after BNP Paribus) worked his way up from a supporting role in an office that monitors trades to a job on the more glamorous futures desk, where he invested the bank's own money by investing in European equity market indexes—making bets on the future performance of the markets. The rogue trader escaped detection by using knowledge of the bank's control systems gleaned in his earlier monitoring job. He got caught when markets dropped, exposing him in contracts in which he had bet on a market rise. His elaborate scheme cost the bank 4.9 billion euros and appears to be the largest trading fraud ever carried out by a single person.[34]

In April 2008, the Financial Industry Regulatory Authority (FINRA) issued a public pronouncement on rogue trading. Regulatory Notice 08–18 provides financial institutions with regulatory guidance and best practices for detecting and preventing unauthorized trading, such as:

- Mandatory vacation policies
- Heightened scrutiny of red flags
- Protection of systems and risk management information
- Need for clearly communicated roles and responsibilities
- Importance of creating a culture of compliance beginning with top management

Auditors can play an important role in identifying rogue trading patterns through their independent and targeted reviews. All too often, rogue trading is a result of stale controls that are not appropriately executed. Auditors should place particular focus on the following areas:

- *Excessive profits:* Generating profits that are significantly above plan may not be good news and can indicate a red flag.
- *Unaligned compensation models:* Gains are rewarded with bonuses while there is no penalty for losses. This encourages risky behavior, as traders have nothing to lose.
- *Unclear functions within trading departments:* There is often a poor differentiation between market making and dealer functions versus proprietary risk taking. This increases the risk of rogue trading.
- *Lack of a true long-term incentive model:* Annual compensation cycle often leads to boom-and-bust results while trading managers or departments do not necessarily understand and challenge how "their" capital is being allocated in the market.
- *Dual responsibilities of trading managers:* Trading managers often maintain a proprietary account, which focuses managers on their account rather than on oversight of the trading floor and involvement in day-to-day activities.

[34] Emma Vandore, "Société Générale Uncovers Massive Fraud by Futures Trader," Associated Press (January 25, 2008).

MORTGAGE FRAUD

Mortgage fraud has quickly become an escalating problem in the United States and a contributing factor to the billions of dollars in losses in the mortgage industry. Mortgage fraud trends reflect the overall downturn in the U.S. economy initiated by the subprime mortgage crisis of 2007. The U.S. stock markets suffered their deepest losses since the 1930s; unemployment increased dramatically; the mortgage loan industry reported a spike in foreclosures and defaults; and financial markets continued to contract, diminishing credit to financial institutions, businesses, and home owners. These combined factors uncovered and fueled a rampant mortgage fraud climate fraught with opportunistic participants desperate to maintain or increase their current standard of living.[35]

Mortgage fraud is commonly perpetrated by materially misstating, misrepresenting, or omitting information relied upon by an underwriter or lender to fund, purchase, or insure a loan. For example, the following fraud scheme resulted in the approval and disbursement of approximately $7.9 million in mortgage loans.

According to the indictment, the alleged organizer of the scheme identified five properties to be used to defraud a mortgage lender, Wells Fargo Bank. A real estate broker negotiated the purchase transactions with the sellers of the properties on behalf of the alleged organizer. The alleged organizer and other recruiters recruited straw buyers to submit fraudulent loan applications to the lender, and paid off title agents to facilitate the closing of the transactions. The alleged organizer and the title agent caused the lender to lend more money than it otherwise would have lent by preparing and submitting to the lender a false HUD-1 Settlement Statement with an inflated purchase price. The defendants then concealed the fraudulent scheme by creating a second version of the HUD-1 Settlement Statement to be provided to the seller reflecting the actual purchase price of the property. At closing, the defendants diverted millions in loan proceeds by skimming the difference between the inflated purchase price and the price actually paid to the seller for the property.

After the closing, the defendants used those loan proceeds to pay off their co-conspirators, including the title company agents, the recruiters, and the straw buyers, and to finance their lavish lifestyles. In some instances, the defendants stripped more money out of the properties by taking out home equity lines of credit, which they used to conceal the fraud by making mortgage payments, and to further enrich themselves. Ultimately, the straw buyers defaulted on the loans, causing each of the properties to go into foreclosure and resulting in probable losses to the lender in excess of $4.5 million.[36]

[35] Federal Bureau of Investigation, *2008 Mortgage Fraud Report,* July 2009.
[36] *United States v. Greta Medina et al.,* December 2009.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 24

Ponzi Schemes

Steven L. Skalak, Regina Lau, and Sherrie Clarke

PONZI SCHEME ORIGIN AND DEVELOPMENT

Ponzi schemes are illegal investment scams that use funds received from subsequent investors to pay returns to earlier investors, rather than distributing revenues generated from any actual business. Promoters of Ponzi schemes often reel in investors by offering high rates of returns over relatively short periods of time. Such scams can continue for some time because of the illusion that investors appear to be getting the returns that they were promised, which in turn encourages new investors to contribute funds and also encourages the reinvestment into the scam by original investors.

Ponzi schemes were named after Charles Ponzi, an Italian immigrant to the United States, who became notorious for using such a scheme to defraud investors. In the 1920s, Ponzi operated an investment scheme though his business, Securities Exchange Co., and promised investors returns of up to 50 percent on the basis of making investments in and arbitraging International Postal Union reply coupons for postage stamps. In theory, at the time it was possible to take advantage of the disparities in international exchange rates and realize huge profits on each transaction. Reply coupons could actually be purchased in Italy for pennies and then converted to postage stamps in the United States worth several times their purchase price. While this business model and its profitability could be demonstrated on a small scale, the mechanics of conducting such a business overseas by transporting coupons and exchanging them for cash caused delays and extra costs, which prevented him from paying investors in the timeframe that he had promised. When Ponzi discovered that he could actually only make a few cents per coupon and that handling large volumes of coupons cost more than they were worth, he stopped redeeming the coupons but continued to collect investors' money.[1] After some initial success in this venture, Ponzi's operation began to encounter significant losses. To keep the scheme running, Ponzi began to divert funds from new investors to repay old investors. Every day, new investors who heard about this new business venture wanted in and handed over their savings. Approximately 40,000 people invested about $15 million in total

[1] Prepared statement of Debra A. Valentine, general counsel for the U.S. Federal Trade Commission, on pyramid schemes.

to the scheme. After a few months, the scheme fell apart as people started to wonder how Ponzi bought and sold what was purported to be 160 million reply coupons out of the 27,000 coupons that existed in the world. The authorities eventually caught on to his operation and busted him. In the end, only about one third of the $15 million was returned to investors.

While Ponzi was not the first to use such a clever scheme, his operation brought in such a substantial amount of money that it was the first to be known throughout the United States. Ponzi was later exposed, jailed, and eventually exiled back to Italy where, ironically, he died penniless, but his name lives on to identify a type of financial fraud that depends on promises of unrealistic profits to investors in the form of high rates of return, and on attracting more and more new investors to provide the funds to repay old investors.

Basic Framework of a Ponzi Scheme

The basic idea behind the operation of a Ponzi scheme is simple. Hook a small amount of investors into believing that they are getting in early on a once-in-a-lifetime opportunity to make huge profits on an investment. This opportunity is such that the investor cannot lose, and only a select few have knowledge of this opportunity. The details of the investment are not very important to the scheme. It is the idea of getting in early on a deal known only to a select few and having the chance to make huge gains that suckers investors into handing over their savings. Investors' greed is the driving force behind the success of a Ponzi scheme.

Once the promoter has roped in a few initial investors, the promoter takes a cut off the top for himself and uses the remaining funds to pay initial returns (which are not real) to the first set of investors. The promoter then seeks new investors to participate in the scheme. Once the second set of investors is in, the funds from those investors are used to pay additional returns to the initial investors. Eventually the second set of investors will need to receive their returns. The promoter then rounds up a third set of investors to pay the second set of investors and to pay additional returns to the initial investors. As this cycle continues, it begins to get more and more complicated to sustain. Initial investors may become suspicious if they do not continue to see returns and the new investors will need to receive returns as well. New investors will have to continuously be added to the scheme for it to keep operating. Eventually, as the scheme grows and as more and more investors are added, the scheme will become unsustainable and inevitably collapse.

Although many victims of Ponzi schemes end up losing large portions of their savings, there are some investors who come out ahead. Early investors who manage to withdraw their funds from the scheme in time may be able to retain their initial investments, and in some cases, come away with considerable gains. Unfortunately, it is the later investors who are certain to lose money.

Types of Ponzi Schemes

Ponzi schemes operate under a variety of names including those such as "high yield investment programs" and "high yield debentures." Their common traits include exceptionally high returns with no underlying business to generate them.[2]

[2] http://moneyterms.co.uk.

Ponzi schemes can vary greatly in length and complexity. Some Ponzi schemes are very basic in nature and involve only the promoters' initial promise to put investors' funds into some form of an investment vehicle. The promoter accumulates more and more money while feeding investors reasons as to why the promised returns cannot be paid right away. The promoter then disappears into the night with all of the cash, never to be seen or heard from again. These types of Ponzi schemes typically last for a short period of time.

Other, more complex forms of Ponzi schemes are more difficult to detect. They may involve an actual investment vehicle that the promoter invests funds into, while pocketing some of the money for himself. The promoter may also invest the money into something other than the investment vehicle that the promoter has explained to investors so that he can generate profits to cover the amount that has been pocketed.[3] Such Ponzi schemes can continue for several years without detection, as you will see in the examples described later in this chapter.

Spotting a Ponzi Scheme: Common Attributes

While Ponzi schemes can vary in several ways, there are a few attributes that are fairly consistent among these types of schemes. For example, Ponzi schemes will usually offer returns to investors that are abnormally high and quite consistent. These investments are often advertised as carrying little or no investment risk. Investors are also provided with very basic account information, if any, on their investments. There is usually a lack of transparency in communications with company management and after some time there may be a sudden stoppage of returns on investment. These are only a handful of signs that may signal that an investment is a Ponzi scheme. However, it should be noted that because an investment stops paying returns or goes out of business, it does not necessarily mean that the investment was a part of a Ponzi scheme.[4]

RECENT SPOTLIGHTS

Ponzi Schemes in the United States

In recent years, Ponzi schemes have become increasingly prevalent in the news as more and more schemes are starting to unravel. The current economic downturn may be, at least in part, the cause. Previously, promoters of Ponzi schemes have been able to reinvest funds received from investors into thriving sectors of the market so they could generate profits to repay investors. Currently, markets are not thriving at nearly the same levels that they once were, which makes it difficult for promoters to generate these profits. Also, tighter lending requirements have decreased other sources of funding, making it more difficult for promoters to keep their schemes afloat. Noted next are some recent schemes to unravel in the United States involving Ponzi schemes.

[3] "OverRegd," securities regulation and litigation blog.
[4] Id.

The Bennett Funding Group, Inc.

In March of 1996 a civil action was filed by the SEC against Bennett Funding Group, its CFO, Patrick R. Bennett, and other companies that Bennett controlled. The companies raised hundreds of millions of dollars, purportedly to purchase assignments of equipment leases and promissory notes.[5] The scheme had over $1 billion of liabilities and 50 known related entities. The $700 million fraud was perpetrated against 245 banks and over 12,000 individual investors.

How did this scheme work? Bennett purchased leases for office equipment such as copiers, faxes, phones, and computers, and then resold them to investors. The leases were marketed as tax-free and safe investments, since the payments for the office equipment generally came from municipalities or federal agencies. Some even had an insurance component that seemed to guarantee the returns. The catch for so many of the victims was exactly that—guaranteed high returns with no risk. Investors received a check every month up until the private, family-controlled company filed for Chapter 11. Other than the fact that they were not registered securities (and thus not filed with the SEC), there was nothing obviously outlandish about the leases. Their returns of around 8 to 12 percent were better than an average municipal bond's.

At first glance, it does not appear that the Bennett operations were a complete fraud. There was a real business upon which the alleged sham was built. The problem, according to the SEC, was that Bennett sold the same leases multiple times to different investors. Some of the leases were pooled together, with the same ones represented in different pools. Others were allegedly entirely fictitious or were pledged as collateral to banks before being sold to investors who were unaware that what they had bought had already been pledged to someone else. By the end of the scheme, Bennett was paying out over $30 million a month to investors but was collecting only about $13 million from actual leases.

On June 26, 1997, U.S. attorney Mary Jo White indicted former CFO Patrick Bennett on 37 counts that include conspiracy, securities and bank fraud, lying to the SEC, money laundering, and concealing assets.[6]

Thomas J. Petters

Minnesota businessman Tom Petters allegedly orchestrated a Ponzi scheme that defrauded $3.5 billion from investors over a 13-year period. The alleged scheme involved soliciting cash from hedge funds, money managers, and grass-roots investors such as church groups to buy high-end consumer electronics for resale at high markups to retailers such as Costco and Sam's Club.[7] According to the SEC, to induce investors to provide the funds, Petters and his co-conspirators made false statements, made material misrepresentations and created false documentation, including purchase orders, invoices, bills of sale, wire transfer confirmations, shipping documents, and financial statements for the purpose of tricking investors into

[5] www.sec.gov/divisions/enforce/claims/bennett.htm.
[6] http://money.cnn.com/magazines/fortune/fortune_archive/1997/08/18/230208/index.htm.
[7] www.startribune.com/business/35326409.html?page=2&c=y.

providing billions of dollars to the scheme.[8] According to authorities, the goods never existed and the investments were diverted to other activities and to fund high-rolling lifestyles.

The Ponzi scheme came to an end when Petters's top co-conspirator turned government informant and wore a wire. On December 1, 2008, Petters was charged with 20 counts of conspiracy, mail and wire fraud, and money laundering. The indictment also charged Petters Group Worldwide, his holding company, and Petters Co. Inc., a financing entity, with all but eight money laundering charges.[9]

Bernard Madoff

On February 9, 2009, a Partial Judgment on Consent Imposing Permanent Injunction and Continuing Other Relief was entered by consent against Bernard Madoff. According to the SEC's complaint, Madoff and Bernard L. Madoff Investment Securities LLC (BMIS) conducted a $50 billion fraudulent scheme through the firm's investment advisory business. In or around early December 2008, Madoff had told senior employees at BMIS that there had been approximately $7 billion in advisory client redemption requests and he was struggling to obtain the liquidity necessary to meet those obligations. When the employees pressed Madoff for more information, Madoff allegedly said that his advisory business was a fraud, "just one big lie [and] basically, a giant Ponzi scheme" that had been paying returns to certain investors out of principal received from other investors. Madoff allegedly said that he intended to surrender to authorities after he paid out remaining money to selected employees, friends, and family members.[10]

On March 12, 2009, Madoff pleaded guilty to 11 federal offenses, including securities fraud, wire fraud, mail fraud, money laundering, making false statements, perjury, theft from an employee benefit plan, and making false filings with the SEC. Madoff's plea allocution stated he began his Ponzi scheme in the early 1990s. He admitted he had never made any legitimate investments with his clients' money during this time; instead, he deposited the money into his business account at Chase Manhattan Bank. He admitted to false trading activities masked by foreign transfers and false SEC filings. To conceal his fraud, he admittedly misrepresented to clients, employees, and others that he purchased securities for clients in overseas markets. To further cover up the fact that he had not executed trades on behalf of his investment advisory clients, he admitted to knowingly causing false trading confirmations and client account statements that reflected the bogus transactions and positions to be created and sent to clients who believed that they had invested in securities through him. Madoff also admitted to concealing the fraud by filing false and misleading certified audit reports and financial statements with the SEC.[11] Madoff told the court his intention had always been to resume legitimate trading activity, but it

[8] http://stmedia.startribune.com/documents/PettersIndictment12_01_08.pdf?elr=KArks:DCiU1OiP:DiiUiacyKUUr.
[9] www.startribune.com/business/35365704.html.
[10] www.sec.gov/litigation/admin/2009/34–60118.pdf.
[11] http://news.findlaw.com/hdocs/docs/madoff/bernard-guilty-plea31209statement.html.

proved "difficult, and ultimately impossible" to reconcile his client accounts. In the end, Madoff said, he realized that his scam would eventually be exposed.

The massive Ponzi scheme run by Madoff since at least the early 1990s demolished the life savings of thousands of people, wrecked charities, and shook confidence in the U.S. financial system. Those affected included individuals, charitable organizations, trusts, pension funds, and hedge funds. U.S. District Court Judge Denny Chin cited the unprecedented nature of the multibillion-dollar fraud when he sentenced Madoff to the maximum of 150 years in prison, a term comparable only to those given in the past to terrorists, traitors, and the most violent criminals.[12]

Stanford International Bank

In February 2009, the SEC accused Texas billionaire Allen Stanford, his college roommate, James Davis, and three of their companies of carrying out a "massive Ponzi scheme" that lasted over at least a decade. They are accused of misappropriating at least $1.6 billion of investor funds and falsifying financial statements issued by Antigua-based Stanford International Bank to investors who bought $8 billion worth of certificates of deposit, whose large returns turned out too good to be true.

According to the complaint, the SEC alleged that by February 2009, Stanford and Davis had misappropriated at least $1.6 billion in investor money through "bogus personal loans" to Stanford. The funds were invested in "speculative, unprofitable private businesses controlled by Stanford," it said. Every month, Stanford and Davis set a predetermined rate of return for certificates of deposit issued by their Antigua bank, then bank accountants reverse-engineered financial statements to "report investment income that the bank did not actually earn," the SEC charged.

The $1.6 billion in loans first came to light in a criminal complaint filed by the Justice Department against Laura Pendergest-Holt, the 35-year-old chief investment officer for the Stanford Financial Group, who was arrested by the FBI in late February. Interviews with former Stanford employees and testimony provided in court documents indicate that over time, top managers surrounded themselves with a team of friends, family, and acquaintances who had little financial experience, but were as close-knit as the small Southern towns from which several of them came. The SEC said these ties created an environment that left "no independent oversight" over the Antigua-based bank's assets (see Exhibit 24.1).[13]

Global Ponzi Schemes

Ponzi schemes not only occur in the United States, but they are also perpetrated in other countries throughout the world. While the impact and severity of penalties assessed for Ponzi schemes may differ by location, the premises are similar to those in the United States. Noted next are a few examples of major Ponzi schemes from outside the United States.

[12] www.huffingtonpost.com/2009/06/29/madoff-sentencing-today_n_222110.html.
[13] www.nytimes.com/2009/02/28/business/28stanford.html.

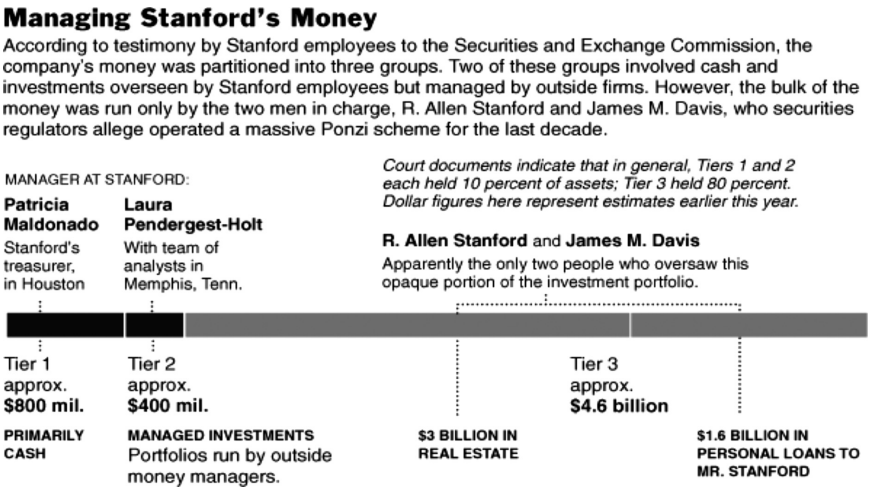


EXHIBIT 24.1 Stanford's Ponzi Scheme
Source: SEC documents.

Albanian Ponzi Schemes

During the 1990s, Albania was in the midst of transitioning from a state-controlled economy to a liberalized market economy. At the time, Albania was one of the poorest and least financially sophisticated European countries. Albania was unfamiliar with financial markets and the economy lacked an adequate formal financial system. Albania's banking system consisted of only three state banks, and those banks held a total of 90 percent of the country's deposits. While these banks offered real interest rates, the Bank of Albania imposed tight credit ceilings on them because of the growing portfolios of bad loans.

Because of the inadequacies of the formal financial system, an informal market soon developed. Informal lending companies were considered safe, and even regarded as making an important economic contribution. Operating alongside these companies, however, were deposit-taking companies that invested on their own account rather than making loans.

Inadequacies in the regulatory framework made it virtually impossible to determine who had the responsibility for regulating the operation of companies in the informal market. Several companies began to operate various investment schemes without any real assets. Some of the larger companies (that is, VEFA, Gjallica, and Kamberi) had substantial real investments to start, and though it is possible that these companies were not schemes from the outset, as described further on, they later became part of the vast Ponzi schemes that swept the country in 1996 and 1997. At the time of their collapse, their liabilities massively exceeded their assets.

In early 1996, two new entities entered the market, Xhafferi and Populli, and offered still higher rates. Accordingly, existing entities such as Sude, stepped up their activities and increased their rates. These rate increases caught the attention of investors and sparked an increased level of interest. In a matter of months, Xhafferi and Populli attracted nearly 2 million depositors between them, in a country with a

population of about 3.5 million. In September, Populli offered more than 30 percent a month. In November, Xhafferi offered to triple depositors' money in three months. Sude responded with an offer to double principal in two months. By November, the face value of the investments totaled $1.2 billion. Albanians sold their houses and farmers sold their livestock so they could invest. These appeared to be can't-lose situations.

Despite repeated warnings from the IMF and the World Bank, the finance ministry did not warn the public about investing in these entities until October. Even then, the warnings gave a false impression of the distinction between legitimate operations with real investments that were solvent and investment schemes with no underlying investments. On November 19, Sude defaulted on its payments and the great collapse began. In January 1997, Sude and Gjallica declared bankruptcy, which triggered riots. By March 1997, Albania was in a chaotic state. As chaos ensued, the government lost control of the south, much of the army and police force had vacated, and 1 million weapons had been looted from armories.

Approximately 2,000 people were killed in the violence that followed the collapse of these investment schemes. Government revenues collapsed as customs posts and tax offices were burned to the ground. By the end of June, the lek had depreciated against the dollar by 40 percent, and prices increased by 28 percent in the first half of 1997 alone. Many industries temporarily ceased production, and trade was interrupted.

In July, the newly elected parliament passed a law, drafted with the assistance of the IMF and World Bank, mandating the appointment of foreign administrators from international accounting firms to liquidate the schemes. The administrators did not gain full control of all of the companies until March 1998. Owners who had not fled were jailed, and whatever assets remained were prepared for sale, much of which had already been lost.[14]

Hoffland Finance

In 1998, Hoffland Finance, of Delhi, India, collapsed amid a major scandal. Delhi police arrested the chairman and managing director (CMD), Deen Bandhu Sharma, of Hoffland Finance, for allegedly defrauding investors of more than Rs 80 crore (800 million rupees). Hoffland enticed investors by offering a whopping 27 percent interest by floating a new company called *Invest Card*. The company, through its various arms, collected more than Rs 150 crore (1.5 billion rupees) from investors and used the funds to speculate in stock markets.[15]

Forum Filatelico and Afinsa Bienes Tangibles

On May 10, 2006, Spanish police arrested nine individuals accused of stealing from customers at two firms specializing in investing in postage stamps. Staff at Forum Filatelico and Afinsa Bienes were suspected of taking a substantial amount of money from approximately 250,000 investors under false pretenses in a fraud dating back

[14] www.imf.org/external/pubs/ft/wp/2009/wp0995.pdf.
[15] www.indianexpress.com/ie/daily/19980508/12850444.html.

between 1998 and 2001. According to a statement by Spanish police, "Potential investors were offered high returns from the purchase and management of a stamp fund, which was apparently made up of overvalued—or even fake—stamps and whose returns did not apparently come [from the fund] but from money received from new clients."

Cash Plus

In 2007, another major Ponzi scheme to make the headlines was that of Cash Plus Limited in Jamaica. Its founder, Carlos Hill, was a Jamaican national who had reportedly worked in the financial sector in the United States in the 1980s. While the details of the scheme appear murky, through his investment scheme, investors received returns of as much as 10 percent monthly.

In 2007, media reports indicated that investors were having difficulty making withdrawals and that Cash Plus's founder, Carlos Hill, had served ten years in a U.S. prison for racketeering, mail fraud, and making a false statement. As a result, in November 2007, the Financial Services Commission (FSC) instructed Cash Plus to provide its investors and the FSC with basic financial information, including details about its assets, liabilities, capital, revenue, and expenses. Cash Plus failed to provide most of the information that was requested. Subsequently, the FSC performed an investigation of Cash Plus and determined that the company as well as Hill and an accomplice, had engaged in securities violations that breached Sections 7, 10, and 26 of the Securities Act. In March of 2008, the FSC announced that Cash Plus had informed it that it did not have the funds to repay investors on March 31, 2008, as planned. Days later, the Supreme Court appointed a receiver-manager from PricewaterhouseCoopers LLP. In April 2008, Hill was arrested on charges filed by the DPP of fraudulent conversion, obtaining money on false pretenses, and conspiracy to defraud. According to the May 2008 interim report by the receiver, between 2004 and 2007, Cash Plus took in investor funds of J$22 billion (US$260 million) from approximately 35,000 to 45,000 investors.[16]

INSIGHTS INTO PONZI SCHEMES: PASSING TREND OR LASTING REALITY?

As you can imagine, very few data exist as to the relative size of Ponzi schemes, and attempting to piece together the facts such as the total amounts invested and lost, or the total amount of investors affected, proves to be an extremely arduous task. This reflects inaccuracy or lack of financial statements and disappearance of funds, among other things. The figures in Exhibit 24.2 reflect data based on public information, as compiled by the International Monetary Fund (IMF). The information available provides useful context. All figures reported are based on public information, and do not reflect estimates by Fund staff or national authorities.

The examples depicted here represent only a portion of the Ponzi schemes that have been in operation in recent years and they reflect a true sense of urgency for

[16] Id.

EXHIBIT 24.2 Some Speculative Data on Selected Investment Schemes

Country	Name(s)	Years in Operation	Promised Rate of Return	Amounts Invested/Lost		Number of Investors/Accounts	
				In U.S. dollars	In percent of GDP	Number 1/	In percent of population
Jamaica	OLINT, Cash Plus, World Wise, LewFam, and so on	2004–2008	6 to 20%/month	1 to 2 billion	12.5 to 25	50,000	2
Grenada	SGL Holdings	2006–2008	7 to 10%/month	30 million	5	...	...
United States	Madoff Investment Securities	2008	10 to 17%/year	50 billion	0.3	13,000	<0.01
Colombia	DRFE, DMG, and so on	2005–2008	300%/six months	1 billion	0.4	Up to 4 million	<8
Lesotho	MKM Burial Society	2007	60%/year	42 million	3	100,000	4
Albania	VEFA, Gjallica, Kamberi, and so on	1991–1997	4 to 19%/month	1.7 billion	79	2 million	57
Macedonia	TAT Savings House	1997	4 to 5%/month	80 million	3	25,000	1
Romania	Caritas	1992–1994	800%/six months	450 million	1.5	2 to 3 million	9 to 13
Russia	MMM	1993–1994	7,000%/six months	1 to 1.5 billion	0.5 to 0.8	1 to 2 million	0.6 to 1.3
Peru	CLAE	1978?–1993	5%/month	200 million	0.3	300,000	1.2
Serbia	Dafiment Bank	1990–1993	15%/month	600 million	...	14 million	133

1. Number of accounts for Dafiment Bank.

Sources: Jamaica, CaPRI (2008); Grenada, newspaper accounts; United States, Securities and Exchange Commission; Colombia, newspaper accounts; Lesotho, Central Bank of Lesotho; Albania, Jarvis (2000); Romania, Verdery (2005); Russia, newspaper accounts; Peru, newspaper accounts; Serbia, newspaper accounts; Macedonia, newspaper accounts.

policies to be put into effect by regulators to help them curtail and eventually prevent these types of schemes from occurring. In reviewing Ponzi schemes of the past and present, it is noted that identifying and forcing the collapse of these schemes is a challenge for authorities for several reasons. In some cases, the promoters or the schemes or both may not be regulated, which makes it difficult for them to appear on the radar of regulators. There is also the fear, by some governments, of being blamed or criticized for triggering the collapse of schemes once they become large. However, once the schemes do collapse, the government may be blamed for failure to detect and notify investors in the early stages of the scheme.[17]

Why Are They Popping Up More Now?

Every day it seems as though regulators are uncovering yet another Ponzi scheme and it appears as though there is no end in sight. But why are Ponzi schemes all of a sudden becoming so popular? Well, the answer has a lot to do with the current state of the economy.

Currently, the economy is in a downturn. Banks and other financial institutions are imposing tighter lending requirements. Markets are not thriving as much as they used to. Investors are pulling portions of their money out of the stock market and placing them into non-risk-bearing accounts such as checking, money market, and other types of savings accounts.

What does this mean for Ponzi scheme promoters? This means that promoters are unable to take investors' money and place it in a booming sector of the market, as these have become few and far between. Therefore, it makes it increasingly difficult for promoters to generate the funds to be used to repay investors. With tighter lending requirements, promoters are less likely to obtain loans from banks to continue to perpetrate their scheme. Added to this, the desire of investors to withdraw funds in order to place them in safer investment vehicles, or for a variety of other reasons, creates a demand on funds that simply do not exist. In scrambling to repay investors, at some point the promoter realizes that she cannot sustain the operation of the scheme and it inevitably collapses.

Ten Red Flags that You May Be Investing in a Ponzi Scheme

Listed here are ten red flags that can alert investors that they may be investing in a Ponzi scheme:

1. Investment manager is unknown, unregulated, comes without good referrals, or hasn't been in the industry for very long. It may be good practice to do some independent research to see whether or not the investment manager has been subject to any negative publicity or has been the subject of any legal actions.
2. Investment manager wants to take complete control of your money, and asks for checks to be made out to him or a company he controls. Your safest bet is to have the funds held separately, in custody at a big broker-dealer firm regulated by the

[17] www.imf.org/external/pubs/ft/wp/2009/wp0995.pdf.

Financial Industry Regulatory Authority (FINRA) and backed by the Securities Investor Protection Corporation (SIPC).

3. Broker "guarantees" investment performance, boasts a track record that looks amazing, or tries to hustle you aggressively into investing. You should double-check any investment record that looks too steady over the long term: Ponzis like to keep the boat steady to avoid redemptions.[18]
4. Fuzzy investment strategy whereby the investment manager either declines to share the strategy or indicates that the details of the investment are so complex that it is difficult to explain. If the investment strategy is unclear, it may be because there isn't one.
5. Small-scale or lesser-known auditing firm used to perform audits of the investment firms' books and records. In a Ponzi scheme, the investment manager may limit exposure to their books and records and may avoid the possibility of independent audits.
6. Investment company is managed or owned by a single individual or the company is tightly controlled. Ponzis like to keep their operations secret.
7. Extravagant lifestyle of the investment manager. Some investment managers will acquire lavish items such as expensive clothes, cars, and homes to make investors believe that by investing their funds, they can achieve similar results.
8. Providing excuses when you attempt to withdraw funds. Promoters may provide excuses because the funds are not readily available or there is no intent to return funds that were received.
9. Lack of investment statements.
10. Sounds too good to be true. As the old adage says, "If something sounds too good to be true, it probably is." It is virtually impossible to generate double-digit returns on an investment year after year, regardless of how well the market may be doing.

Lessons Learned

We see time after time that investors are gullible and chase after returns that are inconsistently high. Especially in tough economic times, many victims can easily fall prey to these get-rich-quick schemes with the hope of making fast and easy money. For some, all it may take is a smooth-talking gentleman, with a great smile and a warm personality, to persuade them to hand over their cash so they can invest in a "great deal." Investors need to come to terms and realize that not every one wins on their investments all of the time. It's a game of chance and the odds are not always in the investor's favor.

Investors should make sure that they perform the proper due diligence before entrusting their hard-earned dollars to someone else. Many investors do not take the time to perform background checks of the individuals handling their nest eggs. Therefore, the investor does not stand a chance in knowing whether or not the promoter is reputable or just another scam artist. As an investor, if you are not sure about the qualifications of the investment manager, your safest bet may be to stick to investing your money with a larger, well-known firm that has been in business

[18] http://online.wsj.com/article/SB122937799268308369.html.

for several years. It is less likely, although not impossible, as we have seen, that an investment company that has been around for years has been operating as a Ponzi. By performing due diligence, the investor may significantly reduce the odds that he or she will become a victim of a Ponzi scheme.

As your mother always told you, don't put all of your eggs in one basket. Investors should consider diversifying their investments. By doing so, the investor can significantly reduce the amount of loss that he may suffer in the event that the investor does become a victim of a Ponzi scheme.

As we have seen in recent history, when economic conditions are stable, Ponzi schemes can thrive and promoters can pay returns. In a downturn, however, as investors seek to withdraw more and more funds, the promoter enters a liquidity crisis, scrambles to find cash, and the Ponzi scheme is exposed.

ACCOUNTANT'S CHALLENGES

Forensic accountants are tasked with the complex duty of unraveling the web of deceit created by Ponzi schemes. The role of the forensic accountant in a Ponzi scheme investigation is to uncover the facts related to the existence and whereabouts of funds and assets and to assist in pursing claims on behalf of investors, counsel, regulatory agencies, trustees, and receivers. The end goal is to locate the cash and return it to investors. This, however, is not as easy as it sounds.

In performing the tasks described earlier, the forensic accountant faces many critical challenges. In the following paragraphs, we will discuss, in detail, some of the major challenges and roadblocks that may be encountered in performing an investigation.

The objective of the investigation is to understand how the Ponzi scheme occurred and how it was covered up. The forensic accountant seeks to obtain an understanding of how the scheme's assets were misappropriated, and whether this occurred through the banks, other financial institutions, through the purchase of other assets, or by any other means.

The forensic accountant should analyze the financial statements of the investment company to attempt to trace the source and location of the funds. We use the word *attempt* here because this process is not an exact science. Financial statements may be nonexistent or may be entirely fictitious, or they may be so tightly woven in with legitimate accounts and transactions that it becomes difficult to separate the two, which presents a major challenge for the accountant.

The use of forensic technology may assist in helping to locate the funds, as data can be recovered from computers and financial data can be reconstructed, preserved, and managed. A challenge here, however, may be jurisdictional laws that may come into play if the data that are to be analyzed are located outside the United States. Many countries have different privacy laws and restrictions that may prevent the accountant from being able to access the necessary data.

The forensic accountant should consider performing interviews of key personnel of the investment company, as this may provide additional insight into how the scheme was structured, and may also provide details as to the whereabouts of the funds. The challenge here is that, in many instances, employees of the investment management company had no knowledge that the company that they were working

for was a scam and key employees may be reluctant to share the details of the fraud that they perpetrated, or they may hold back information.

Another challenge of the investigation team is determining whether any previously paid investors should return all or a portion of the money they received to compensate those owed money at the time the scheme collapses. Since the core attribute of a Ponzi scheme is that early investors are paid off with the money invested by later entrants, it is only natural that the latter class of investors should want something back from those who get out early. These so-called clawbacks are discussed further on. The challenge with this type of analysis and indeed virtually any exercise that seeks to match sources of cash with uses of cash is the fungible nature of cash as an asset. Once cash is deposited with other funds, it is virtually impossible to say which deposit was used to make any individual disbursement. Nevertheless, a careful matching exercise, in which available balances immediately before and after individual receipts and disbursements, may illuminate how funds were used by the fraudsters to keep enough investors happy to maintain the scheme.

This type of analysis frequently involves the laborious recreation of transactions from bank statements and other records. It is often greatly aided by forensic technology to assist in manipulating the data in a variety of analyses to show where funds received were applied.

REGULATORY BODIES AND TASK FORCES

Since 2003, the SEC has settled with more than 300 defendants alleged to have been involved in Ponzi schemes. Sixty-two settlements have related to 12 cases in which the alleged Ponzi scheme raised at least $50 million. These cases are summarized in Exhibit 24.3. While it is clear from the figure that the SEC settlement amounts in these cases are generally small, it is important to note that many of the cases are young and that recoveries obtained through criminal actions or private litigation are not included.[19]

Regulatory Response

The SEC has taken action against a large number of Ponzi schemes in recent years through the assessment of heavy fines, ordering disgorgement of profits, and obtaining prison sentences for the offenders, among other things. Such schemes have come to the SEC's attention through a variety of sources such as whistle-blowers, investor complaints, media reports, and so on. The SEC conducts investigations of the investment managers and companies that are the subject of allegations, and in many cases seeks restraining orders, freezes of assets, and the appointment of receivers.

In the past, the primary authority for the regulation of investment managers and companies rested with SEC. As this chapter was being written, changes were being made to this structure. In November 2009, President Barack Obama announced the creation of an interagency task force to combat financial fraud. This task force will be led by the Justice Department, and will include representatives from the SEC,

[19] www.nera.com/image/PUB_Ponzi_Schemes3_0309_final.pdf.

EXHIBIT 24.3 SEC Settlements in Alleged Ponzi Schemes Involving at Least $50 million in Investor Funds Since 31 July 2002

Investment Agent	Complaint Year (1)	Alleged Fraud Size ($ mil) (2)	SEC Settlements to date ($ mil) (3)	# of Defendants Settled with by the SEC (4)	Alleged Fraud Duration (Years) (5)
Mutual Benefits Corp.	2004	$1,067	$110	16	10
Michael E. Kelly et al.	2007	$428	$0	11	6
VesCor Capital Corp.	2008	$180	$0	1	16
Michael J. McNaul et al.	2008	$156	$0	11	4
Private Capital Management, Inc.	2004	$145	$112	4	8
ETS Payphones, Inc.	2002	$96	$0	3	3
Gregory N. McKnight et al.	2008	$72	$0	2	2
Mobile Billboards of America, Inc.	2004	$61	$2	4	4
IPOF Fund	2007	$50	$0	1	6
Real Estate Partners, Inc.	2007	$50	$0	5	4
Tri Energy et al.	2005	$50	$0	6	3
Randal T. Treadwell et al.	2004	$50	$0	4	1

Note: Excludes cases with complaints filed pre-SOX.

the Treasury Department, the Department of Housing and Urban Development, and other agencies.

The Financial Fraud Enforcement Task Force will replace the task force created by President George W. Bush (Corporate Fraud Task Force), which was created in 2002 to investigate major corporate scandals such as WorldCom and Enron. The mission of this task force is not only to hold accountable those who have contributed to the financial meltdown, but also to prevent another meltdown from occurring.

BANKRUPTCY IMPLICATIONS

Many Ponzi scheme cases end up in bankruptcy as investigating teams try to sort through the *who*, *what*, *when*, *where*, and *how* of these operations and determine if any funds can be recovered and returned to investors, creditors, and others. Recent Ponzi schemes have involved business activities including Internet technology; foreign exchange; the offering of notes, loans, and credit facilities; the sales of securities; and futures trading.[20] Some of the implications of cases that end up in bankruptcy are noted next.

[20] Ponzi Scheme Fact Sheet, March 31, 2009.

Clawback Rules

The term *clawback* is used to identify a type of claim that can be declared by a bankruptcy trustee to recover money paid out to investors in a Ponzi scheme before the scheme was revealed. The purpose of a clawback in this context is to recover monies that were transferred out of the debtor's estate (often composed of funds from the fraudulent scheme) before the scheme was discovered and return those monies to the bankruptcy estate so that they can be distributed to creditors—that is, the victims of the fraudulent scheme—in accordance with the priorities established by the Bankruptcy Code. Clawback claims come in two types: preference actions and fraudulent conveyance actions.

A preference occurs when the promoter of the scheme transfers assets (that is, pays someone close to the time of the bankruptcy), allowing the person to be treated better (preferentially) than others. The trustee can look back 90 days for most people who received assets and up to a year for family members or other insiders who received the same. This law is intented to treat creditors equally in bankruptcy.[21]

A fraudulent conveyance occurs when the person who gets something did not give something of comparable value for it (that is, the supposed profits paid out to some investors are not really profits at all, but are taken by the promoter from the investment principal of other investors). The basic rule is that withdrawals of fictitious profits have to be returned to the bankruptcy estate, whereas redemptions of principal do not, unless the investor knew or should have known of red flags at the time of the transaction.[22]

Investors who are in a net loss position are generally not subject to clawback because they are unlikely to have received other people's principal. Investors who are in a net gain position may be subject to a claim under federal or state law for return of any profits they withdrew from the scheme. The look-back period is six years for fraudulent conveyances under New York State law.

SUMMARY

Ponzi schemes are a common form of fraud that attack victims' desires to earn a high return on their money. They are effective in both good and bad times in preying on people's concerns about their relative economic status and earnings. For the forensic accountant, they represent a major challenge to untangle, often requiring the full extent of forensic tools—transaction analysis, interviewing, forensic technology skills, and close coordination with legal teams.

[21] www.eugenebankruptcylawyer.com/blog/2010/08/what-is-a-bankruptcy-preference/.
[22] www.theworldlawgroup.com/docs%5CUnited%20States-Clawbacks%20in%20the%-20Aftermath%20of%20Madoff.pdf.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 25

Money Laundering

Andrew P. Clark, Marie-Alice Hofmaier, and Christopher Cowin

Money laundering within the United States alone, let alone in other parts of the world, remains a serious problem. Exhibit 25.1 conveys a sense of the dimensions of the problem. In fiscal year 2009, for example, the Internal Revenue Service obtained more than 1,000 indictments and over 700 sentencings.

This chapter introduces a range of circumstances in which money laundering may be encountered in business. It examines the relationships and distinctions between fraud and money laundering as well as the remote likelihood of indications of money laundering showing up in the course of a financial statement audit. The chapter looks at the unique skills and perspectives necessary to successfully investigate money laundering and identifies some of the potential red flags a financial statement auditor may encounter if money-laundering transactions are taking place. For the purposes of this chapter, *money laundering* refers to the crime or activity of moving funds of illicit origin, and *anti–money laundering* (AML) refers to formal and informal systems and controls designed to prevent or frustrate attempts to launder money and to report incidents of money laundering when they are suspected or detected. In many jurisdictions, AML systems and controls now also extend to cover counter-terrorist financing (CTF).

While most companies or institutions could potentially be used as conduits for money laundering, AML is of particular concern for institutions in the regulated financial services sector, in which many entities are legally obliged to introduce and maintain AML systems and controls. The distinction between the regulated financial services and unregulated sectors is addressed later in the chapter.

RELATIONSHIP BETWEEN FRAUD AND MONEY LAUNDERING

Although both fraud and money laundering are crimes based on deception and although the movement of funds obtained by fraud is a type of money laundering, fraud and money laundering are distinctly different and should not be confused. Money laundering has been defined in a number of ways, but essentially, it is a process undertaken by or on behalf of criminals with the object of hiding or disguising their criminal activities and the origin of their illicit proceeds. The goals are often achieved through a series of financial transactions, sometimes involving a number of countries and through a variety of financial products.

EXHIBIT 25.1 Statistical Data: Money-Laundering Enforcement

Money Laundering Investigations	FY 2009	FY 2008	FY 2007
Investigations Initiated	1341	1422	1678
Prosecution Recommendations	1048	1305	1275
Indictments/Informations	936	1200	1017
Sentenced	753	686	758
Incarceration Rate*	85.9%	84.7%	87.9%
Average Months to Serve	72	67	62

*Incarceration includes confinement to federal prison, halfway house, home detention, or some combination thereof.
Data Source: Criminal Investigation Management Information System.
Source: Internal Revenue Services, www.irs.gov/.

The Financial Action Task Force (FATF) of the Organisation for Economic Co-operation and Development (OECD) has defined money laundering as follows:

> *The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.*[1]

The FATF is a 34-member intergovernmental body established by the 1989 G-7 Summit in Paris. It has primary responsibility for developing worldwide standards for AML and CTF. It works in close cooperation with other key international organizations, including the IMF, the World Bank, the United Nations, and FATF-style regional bodies (FSRBs). Its primary role is to monitor the development of AML strategies in member countries—although it also seeks to educate both members and nonmembers about the risks of money laundering at the national and international levels. For example, every year the FATF considers money-laundering trends and vulnerabilities and issues a report of case studies summarizing its findings.

Between 2001 and 2006, FATF ran an initiative on noncooperative countries and territories (NCCTs). Twenty-three jurisdictions were listed as NCCTs over the period because they lacked an effective AML/CTF system. This acted as an incentive to them to strengthen their AML and CTF procedures.

Since then, FATF has continued to work toward identifying jurisdictions with AML/CTF deficiencies. When such jurisdictions are identified, FATF issues statements expressing concerns about them. These statements call for enhanced scrutiny on the part of FATF member countries when dealing with jurisdictions with deficiencies. If necessary, FATF can call for countermeasures to be applied to protect the financial system. Regulated institutions in FATF member countries are expected to take FATF recommendations into account.

[1] Financial Action Task Force, "Basic Facts about Money Laundering," www.fatf-gafi.org.

The money-laundering process has been characterized as consisting of at least three distinct stages: placement, layering, and integration. These stages are often referred to as the *money-laundering triad*.

Placement

This initial stage is considered by many as the riskiest part for criminals to achieve as they attempt to introduce the proceeds of a crime into the financial system. Although banks have been used for facilitating this stage in the past—for example, by narcotics traffickers making cash deposits at local branches—the banks' AML systems and controls have become and are perceived to be increasingly sophisticated, and launderers have sought alternative means of placing their illicit cash. One such method is to infiltrate cash-intensive businesses—such as restaurants and other public venues—to provide a plausible explanation for the movement of large amounts of cash. The regulation of casinos, for example, responds to a perceived vulnerability to money laundering.[2] When this scheme succeeds, dirty money is commingled with income derived from the legitimate business and deposited with a bank.

Financial fraud, by contrast, may not necessarily have a placement stage in the conventional sense. The funds may already be in the financial system, particularly when a financial institution has been defrauded.

Layering

Once the cash has been successfully placed in the financial system, the launderer typically initiates a number of related transactions with a view to obscuring the origin of the funds by undermining any trace of an audit trail. That is often achieved by moving the funds between financial products, between institutions, and between jurisdictions.

Integration

Finally, the laundered funds need to be extracted from the financial system so that they can be used to acquire legitimate assets or finance further criminal activities. At that point, the funds or assets have a veneer of respectability within the legitimate economy. Successfully laundered funds may be integrated back into the economy in three ways: by being invested, lent, or spent. Although investing and lending are similar, keep in mind that funds lent to a third party enter the economy in the name of the third party and become more difficult to trace.

Two important characteristics of money laundering distinguish it from fraud. The first is that because of the conduit phenomenon, money laundering is far less

[2] Financial Action Task Force, *Review of the FATF Forty Recommendations* (Paris, May 30, 2002), Chap. 5, § 5.1.1, "Casinos: Vulnerability to Money Laundering," par. 237, 81. According to the FATF, the large amounts of cash being circulated by legitimate customers provide effective covers for the launderer. A more recent typologies report by the FATF discusses the gaps in AML coverage in this sector. Financial Action Task Force, *Vulnerability of Casinos and the Gaming Sector* (March 2009).

likely to affect financial statements than the broad spectrum of frauds is. Hence, it is highly unlikely that financial statement auditing procedures will identify or even stumble onto possible indications of money laundering. The second important distinction is that fraudulent activity often results in the loss or disappearance of assets or revenue from the business, whereas money laundering may actually create significant fee income because businesses may charge fees for the transactions that permit the illicit proceeds to be distanced from their source. Nevertheless, many conditions and control deficiencies that may contribute to fraud vulnerability may also contribute to money-laundering vulnerability—that is, the risk of criminal activity going undetected. Prominent among these are the following:

- Lack of a strong control environment
- Lack of a strong regulatory compliance function, in the absence of which a business is subject to high compliance risk and reputational risk
- Lack of well-defined and well-communicated enterprise-wide ethical guidance and standards and related training programs
- Lack of a robust internal audit compliance program
- Compliance problems, control deficiencies, or concerns over management's competence or integrity or both, raised in previous examiners' or auditors' reports, memorandums of understanding, and past administrative and enforcement actions
- Significant revenues stemming from or assets or liabilities associated with high-risk jurisdictions—notably, bank secrecy havens
- Abnormally high electronic funds transfer activity from and to high-risk jurisdictions—with insufficient controls
- Lack of background checks on new employees
- Unreasonably infrequent or nonexistent reviews of security software and systems

COUNTER-TERRORIST FINANCING

Terrorist financing and money laundering have much in common. Similar methods are often used to achieve both ends. Also, many terrorist organizations are known to have links with organized crime because this helps to fund their activities. There are, however, two major differences between terrorist property and criminal property, more generally:

1. Often, only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property.
2. Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.[3]

[3] JMLSG, *Guidance Notes*, Part I, Preface, par. 9.

Terrorist organizations often control property and funds from a variety of sources and employ modern techniques to manage these funds and to move them between jurisdictions.[4]

VARYING IMPACT OF MONEY LAUNDERING ON COMPANIES

Both fraud and money laundering may result in criminal penalties, but perhaps equally significant to companies and financial institutions is the reputational risk associated with those activities. The media interest in Enron, WorldCom, and other massive frauds in years past is indicative of the public appetite for stories involving crime and big business. Whenever such a story breaks, it is often difficult for the company under siege to manage the public relations impact. Not only can share prices fall dramatically, as in the Bank of New York money-laundering case in the late 1990s, but in recent years, the regulators have greatly increased the level of the fines imposed. For example, Credit Suisse was fined $536 million in December 2009 for failure to comply with the OFAC (U.S. Treasury Office of Foreign Assets Control) sanctions regime. Also, any investment by a company in building its brands may be at risk. These issues are addressed in greater detail later in the chapter.

The extent to which a company, its board of directors, and its senior management are focused on money laundering is guided in part by whether or not the company is regulated. The extent to which a company or institution *must* have specific AML systems and controls depends on whether its industry or sector or both is regulated for AML purposes. Today, the degree of regulation still varies considerably among AML regimes around the globe. Historically, the regulated sector has been limited to the banking community. It has been widely acknowledged for some time that banks are on the front line in the fight against money laundering. Over time, and in many jurisdictions, however, the regulated sector has expanded to include nonbanking financial institutions—like insurance companies, investment managers, and other participants in the financial sector—stemming in large part from the conventional wisdom that money launderers tend to move their operations into channels where they believe their illicit activities are likely to go undetected.

AML regime expansion across financial services sectors is a primary characteristic of the PATRIOT Act of 2001 (the Act), unquestionably the most sweeping piece of AML legislation in U.S. history.[5] The act is applicable to U.S. institutions and to foreign entities with U.S. operations. Congress also sought to shore up perceived weaknesses in the existing AML regime through renewed attention to the regulation of offshore banking, correspondence banking relationships, and private banking services.

Allied with the conviction that the AML environment needed change was the perception that previous efforts had been impeded by inadequate legislation and

[4] JMLSG, *Guidance Notes*, Part I, Preface, par. 10.

[5] PATRIOT is an acronym. The short title of the act is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. The portion of the act that relates to AML is Title III, International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

enforcement powers, particularly in cases involving foreign persons, foreign banks, and foreign countries. To this end, the act widened the AML regime to incorporate the nonbanking financial sector, including investment managers and broker-dealers. Further expansion of the regulated sector to cover nonfinancial institutions, including accountants, is addressed later in this chapter.

If a company is regulated for AML purposes, it is likely that, at a minimum, the company needs to introduce systems and controls designed to minimize and frustrate money laundering. Although the particular requirements vary by jurisdiction, there are seven main areas that regulated institutions often need to address to varying degrees. The purpose of underlying programs that incorporate these several areas is to know your customer (KYC). These also allow the monitoring of transactions so that unusual transactions can be pulled out of the normal processing flow either before or after they are executed. This permits further inquiry when required.

THE FIVE-POINT PROGRAM FOR AML-REGULATED BUSINESSES

Written Compliance Program

Businesses should have a regulator-approved AML policy framework, enterprise-wide guidance and standards, implementation policies, and robust operating procedures that integrate compliance into the business and into support areas of consequence. The written AML compliance program should clearly articulate mechanisms for discharging business unit and individual AML responsibilities. The institution is also expected to consider appropriate controls to authorize policy and procedural variances. There is an expectation that the institution should carry out and document its own risk assessment—that is, its own assessment of the vulnerability of its products and services to money laundering and the corresponding controls that have been introduced to mitigate these risks. Institutions are also expected to transform risk assessment into a continuous and sustainable process.

Minimum Standards of Customer Due Diligence

The AML requirements also stipulate the circumstances in which customers or counterparties need to be identified and the extent to which identity needs to be verified and documentation reviewed. The documentary requirements should vary according to the type of customer—for example, the requirements for an offshore trust may be tougher than those for a private individual—and the extent to which the immediate customer is acting on behalf of another. In addition, KYC principles have come to apply to employees, vendors, agents, and other external service providers.

The United Kingdom's Joint Money Laundering Steering Group (JMLSG) produces some useful guidance on AML and CTF for regulated financial institutions. Topics covered include politically exposed persons (PEP) and sanctions.

Politically Exposed Persons The term *politically exposed person* has arisen from PEP's history of association with corruption to the extent at which such a

person's presence in a transaction has become a risk indicator. PEPs are persons who have been entrusted with prominent public functions, and people close to such persons.

PEP status itself does not, of course, incriminate individuals or entities. It does not necessarily prevent a firm from doing business with PEPs. It does, however, put the customer, or the beneficial owner, into a higher risk category.[6]

It is therefore recommended that firms apply enhanced due diligence, on a risk-sensitive basis, to PEPs. This would generally include:

- Having appropriate risk-based procedures to determine whether a customer is a PEP
- Obtaining appropriate executive committee approval for establishing a business relationship with such a customer
- Taking adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or occasional transaction
- Conducting enhanced ongoing monitoring of the business relationship[7]

Sanctions Recent years have seen a significant number of economic sanctions being issued, in a number of different forms.

- The Office of Foreign Assets Control (OFAC), part of the U.S. Treasury, operates three programs: country; specified foreign government officials and other persona non grata; and specified individuals, entities, and vessels. The United Nations and the European Union can designate individuals and organizations to be sanctioned. These are individually implemented by countries (for example, by HM Treasury in the United Kingdom).
- The United Nations also calls on members to prevent and suppress the financing of terrorism, and specifically in relation to Osama Bin Laden, Al-Qa'ida, and the Taliban.
- The United Nations also maintains country-based financial sanctions targeting persons and entities connected to the political leadership of targeted countries.
- Trade sanctions, such as embargoes on making military hardware or know-how available to certain countries, can be imposed by countries.
- Countries can add their own sanction targets as well.
- The general form of the sanctions is an asset freeze prohibiting any dealing with the funds or economic resources of the sanctioned party, or making funds or economic resources available to them, or for their benefit.
- A breach of a sanction is likely to be a criminal offense.
- Firms in the regulated sector therefore usually use automated screening solutions to screen their customer base for sanctions compliance.

[6] JMLSG, *Guidance Notes,* Part 1, par. 5.5.18.
[7] JMLSG, *Guidance Notes,* Part 1, par. 5.5.25.

Activity Monitoring and Reporting

After accepting a customer or counterparty and opening an account, the institution is likely to have an obligation to monitor customer activity for evidence of money laundering and, depending on the AML regime, other reportable suspicious conditions. When money laundering is identified or suspected, a report should be made to an appropriate external authority. In many jurisdictions, the relevant external authority is the nominated Financial Intelligence Unit (FIU). There are now more than 100 national FIUs globally, and most of them are members of the international FIU union, the Egmont Group.[8] Although there is a common requirement to report to a nominated authority, the specific role of the FIU varies, depending on a number of factors that are, in turn, functions of the technical and legal framework established for the unit and the FIU infrastructure that has been created. While some FIUs may simply collate and analyze information received and then forward it to another authority for investigation, others play a more active regulatory role in the administration of the country's AML regime. The FIU is often responsible for undertaking compliance examinations, issuing fines and penalties, providing disclosure information, and drafting regulations. The U.S. Financial Crimes Enforcement Network (FinCEN) is both an AML policy-making and enforcement agency. FinCEN's mission is to enhance U.S. national security, deter and detect criminal activity, and safeguard financial systems from abuse by promoting transparency in the United States and international financial systems.

Training

As well as documenting its approach to AML in its policies and procedures, the institution should ensure that AML policies and procedures are communicated to staff through training on a regular basis. Training is likely to cover obligations under the law, circumstances that could indicate that products and services are being used for money-laundering purposes, and when and to whom suspicions should be reported. AML training needs to be tailored to the needs and circumstances of the trainees and to be continually refreshed and tracked.

Record Keeping

Finally, the institution should be mindful of the legal requirements concerning the storage and retention of AML-related documents. The document retained should include evidence obtained when verifying customer identity, suspicious transaction reports made internally, reports submitted externally to the FIU, and records of training.

In certain jurisdictions, AML obligations go even further. In Germany and Switzerland, for example, auditors have an obligation to monitor and report on

[8] The larger, better-funded FIUs include the Financial Crimes Enforcement Network (FinCEN) of the United States, the United Kingdom's Serious Organised Crime Agency (SOCA), France's Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins (Tracfin), Canada's Financial Transactions Reports Analysis Centre (FinTrac), and Australia's Australian Transactions and Reports Analysis Centre (AUSTRAC).

a bank's compliance with AML legislation and regulation. In the United States, the obligation lies primarily with the business.

Within the regulated sector, customers, products and services, channels, and service providers have their own profiles of AML risk. Banking relationships, for example, are likely to be higher risk because they facilitate regular receipts and payments to third parties without the verification of the third party. That risk is magnified when wire transfers and transfer through the Internet are available, because funds can then be moved between jurisdictions. At the other end of the risk spectrum are products involving small regular payments that are repayable only to the account holder and products including certain insurance contracts and personal investment plans, among other instruments. Although no institution is immune to money laundering, its AML policies, procedures, systems, and other controls should realistically correspond to the money-laundering risks posed.

The company's regulated status will inform its general attitude toward money laundering, AML, and financial crime. Some financial institutions have appointed directors responsible for financial crime, including fraud and money laundering. In the United States, AML compliance officers are legally required at covered financial institutions.

A company's regulated status and the attitude of the board and senior management—that is, the tone at the top—have an impact on the extent and quality of the control environment. At a minimum, AML compliance should respond to regulatory requirements. In more sophisticated organizations, those responsible for AML are typically informing other aspects of the business, such as acquisition strategies, introduction of new products and services, entry into new distribution channels, and development and deployment of new technologies.

All of these factors should have an impact on the ability of the financial auditor, forensic accounting investigator, and regulator to assess the impact of money laundering on a business. In the United Kingdom, for example, the company officer responsible for money-laundering matters, including compliance and reporting—the money-laundering reporting officer, or MLRO—has an obligation to annually prepare and deliver to management a report that deals with a number of matters related to money laundering and AML. This is an important document for identifying any problems the organization encountered during the period, but more significant, it is an indication of the organization's and management's attitude toward the issue.

Although a great deal of attention has been paid to money laundering through the movement of funds in the regulated sector, it is important to recognize that nonfinancial companies, too, can be used in money-laundering schemes. For example, in some situations, the movement of goods and services is used as a front for money laundering or as an actual money-laundering mechanism.

It has been argued that customs officials are in a position to identify such suspicious activity by comparing the amount paid with the nature of the goods imported, but there are several barriers to the detection of this type of money laundering.[9] First, duty is often paid on the items being shipped so as to add another layer to the veneer of legitimacy around the transaction. The duty paid is viewed by the criminals as just

[9] Financial Action Task Force, *Report on Money Laundering Typologies 1999–2000* (Paris: February 3, 2000), 10–ep11.

another cost of doing business. Second, importing as a means of money laundering is often not addressed in the training of customs officials in many jurisdictions. The focus of customs officials' training has usually been on uncovering contraband or attempts to avoid paying import duties.

The point here is that while the regulated sector has more obligations than any other in relation to AML, no company or institution is immune to money laundering and money launderers. The challenge for business managers is to evaluate the risk profile of the company in question and to understand where it could be exposed to money laundering—internally or externally.

IMPACT OF MONEY LAUNDERING ON FINANCIAL STATEMENTS

The impact of money laundering on financial statements should be considered in terms of both direct and indirect consequences on fairly representing the state of a business. While the direct impact is clearly important, the indirect consequences can be just as significant—and they are often underestimated by management.

Money launderers tend to use the business entity more as a conduit than as a means of directly expropriating assets. For this reason, money laundering is far less likely to affect financial statements than is a fraud such as asset misappropriation. It is consequently unlikely to be detected in a financial statement audit. Also, other forms of fraudulent activity usually result in the loss or disappearance of assets or revenue, whereas money laundering involves the manipulation of large quantities of illicit proceeds to distance them from their source quickly and without drawing attention.

Although money laundering rarely has a direct impact on financial statements, it may have other consequences of concern. The consequences could be any of the following:

- *Law enforcement interest.* Law enforcement agencies may act on the suspicion that a business has been infiltrated by money launderers. A significant amount of time can be expended responding to requests from law enforcement agencies, ranging from discovery requests and disclosure orders to asset-freeze orders.
- *Regulatory revocation.* A financial services business could have its license and charter revoked in the event that a significant breach in its AML systems and controls is discovered.
- *Operational catastrophe.* There is also the possibility of civil seizure of assets or shareholder derivative suits when it is determined that the institution was negligent in its duties and facilitated the movement of funds.
- *Reputational damage.* Perhaps the most significant implication for an institution is the reputational risk accompanying the incidence or even the allegation of money laundering. This combination of the respectable and disrespectable, of business and crime, is an attractive proposition for the media. Also, the discovery of money laundering at an institution could undermine the trust of previously loyal savers and investors, prompting them to look elsewhere. A brand in which significant resources have been invested could be harmed if money laundering is alleged or discovered.

In summary, although money laundering may not have a direct impact on financial statements, it has the potential to expose a company or financial institution to considerable risk.

AML AND FORENSIC ACCOUNTING INVESTIGATION

When money laundering is suspected or controls are considered vulnerable to abuse, a forensic accounting investigator with the requisite knowledge of AML may be engaged to undertake an investigation, a compliance diagnostic, or a controls review. Many money-laundering investigations begin with a detailed review of transactions and documentation related to specific customers, rather than with high-level controls. From such a process, the forensic accounting investigator charged with executing the review generally will form a bottom-up view of the controls environment and ascertain whether it is consistent with the regulatory regime governing that jurisdiction. Although the scope of AML assignments is determined on a case-by-case basis, in practice all three aspects—investigation, compliance diagnostic, and controls review—are likely to be reflected to varying degrees. The assignments themselves are likely to come from one of two sources: at the request of the regulator or of the institution. These assignments are distinctly different from financial statement audits in that they focus specifically on compliance with relevant laws and regulations as well as on particular suspicious transactions and not on financial accounting processes or the entity's reported financial results.

At the Request of the Regulator

The regulator may seek the involvement of a forensic accounting investigator for a variety of reasons: The regulator could suspect that the institution has perpetrated financial crime or been the victim of financial crime and accordingly authorizes an investigation. Alternatively, the regulator could request an AML review before it is willing to grant a financial license or authorization. The regulator could also request a review as part of a wider but more routine examination of an institution's systems and controls.

Law enforcement officials may also investigate whether an institution was aiding and abetting money laundering through systemic deficiencies or major control failures that permitted the money-laundering activity to remain undetected. Faced with a challenge of that kind, the institution may wish to engage forensic accountants with specialized AML knowledge.

At the Request of the Institution

Of its own volition the institution could engage a forensic accounting investigator to undertake a money-laundering investigation assignment. One of the more common instances is a review in advance of a regulatory visit to identify areas that may need to be addressed. The institution, however, may also require a money-laundering review as part of a wider strategic-vulnerability assessment. A review also may be appropriate in conjunction with an acquisition. The assignment could involve a review of the target's systems and controls or an assessment of the risk profile of its

customer base to determine whether any pricing adjustments to the proposed deal might be appropriate.

In the course of an AML review, a forensic accounting investigator may need to consider all five of the areas that make up the typical AML system and controls, ranging from policies and procedures and customer due diligence to monitoring and reporting, training, and record keeping. All of these areas could enter into a thorough AML review, starting with a detailed examination of transactions and records and concluding with an assessment of the overall corporate culture.

Review of Transactions and Records

Transactions are reviewed or tested for purposes of confirming a number of different aspects of the control environment.

- *Account-opening procedures*. Is the requisite documentation obtained?
- *Exception procedures*. Are departures from policies and procedures signed off by an appropriately senior member of staff? Are the reasons documented?
- *Transaction monitoring*. Is suspicious or unusual activity identified?

This stage of the review addresses aspects of the customer due diligence and record-keeping requirements but may also indicate whether staff have been suitably trained and comply with the employer's policies and procedures.

Decision Making

The decision-making process typically is reviewed at a number of levels, from the application of customer acceptance procedures and departures from accepted practice to the role of compliance and the role of other units of the business, such as internal audit. Investigations in this area often build on the results of the review of transactions—for example, in the areas of exception procedures and feedback from management. Examination of decision making often sheds another light on customer due diligence and policies and procedures, but even more significant, perhaps, on record keeping.

The AML Reporting Process

The reporting process can be addressed from a number of angles.

- By tracing the progress through the organization of suspicious or unusual activity reports made by staff, with the associated record of outcomes and justifications for acceptance or rejection
- Through analytical review of reports—forwarded for consideration by the relevant FIU—that compare the institution with its peer group and with national averages for companies of comparable size
- By looking at the scope of reportable conditions identified through the aforementioned benchmarking process
- By measuring the frequency of reports to and from the MLRO or other relevant compliance officers

This part of the money-laundering review is often concerned primarily with the monitoring and reporting processes but also covers record-keeping and training requirements.

Corporate Culture and AML Corporate Governance

Finally, a money-laundering review should consider the corporate culture and the tone at the top—that is, the extent to which the organization takes AML seriously. The degree of commitment is often reflected in the quality of training the institution provides, and a variety of methods can be used to examine this variable. A sample of training records can be reviewed to identify evidence of attendance at training sessions covering the subject of money laundering, including the frequency and scope of training given. Review of the sample records can be supplemented by discussions with staff to confirm attendance at training sessions and question staff's evaluation of the training and its key messages. The training material itself can be reviewed for relevance. Is it part of a wider, ongoing training and awareness program for staff? Finally, the corporate culture is also indicated by the extent to which the most senior members of the board focus on the issue of money laundering. For example, do the minutes of board meetings show that AML matters are being discussed? Has remedial action been taken to address any weaknesses? Fundamentally, senior management is responsible for raising AML matters with the board when, in management's judgment, a serious problem has arisen or may possibly arise. Many of the AML compliance failures of recent years have been attributed to a board's failure to notify and seek counsel.

LEGAL ARRANGEMENTS LENDING THEMSELVES TO ANONYMITY

Corporate entities may be victims of money laundering, but as noted earlier, corporate entities may also be created and used for the sole purpose of money laundering. Falling between these two extremes are legitimate companies that are unwittingly exposed to money laundering by the activities of someone or some group of conspirators in their organization. This category includes the large multinational entity with a subsidiary infiltrated by organized crime but also includes dishonest bank clerks who accept money they know to be illegitimate, possibly in return for bribes or other perks.

Increasingly, and disturbingly, corporate entities are being used by criminals as integral components in sophisticated money-laundering operations. Corporate entities are attractive for a number of reasons—primarily, the degree of anonymity afforded by complex corporate structures and legal arrangements. That anonymity is useful in avoiding or defeating the inquiries of financial institutions into the true ownership for purposes of assessing who the customer is and the type of business conducted. The lack of transparency is driven by two things: the scarcity of shareholder information in certain jurisdictions and the characteristics of certain legal arrangements that lend themselves to anonymity—in particular, the availability of bearer shares, nominee directors, and certain so-called international business companies (IBCs).

Bearer shares facilitate transfer of ownership of a company through the physical transfer of the share certificate from one individual to another. Unlike ordinary shares, details about the owner are not registered with the company. According to the FATF, these instruments are attractive to money laundering because assets can be transferred without leaving a paper trail—that is, they are highly negotiable instruments—and companies can be owned and controlled without interests being declared.[10]

A nominee director is an officer of the company who is employed to act on behalf of another, either a shadow director or the beneficial owner. The nominee director may be an individual or corporation, and that name is often the only one that appears on documentation filed with the relevant registries. The problem with nominee directors is that they undermine the value of obtaining information about the company and, like bearer shares, potentially enable someone to effectively control a company without declaring an interest. It is also possible to use corporate nominee directors to lengthen the chain of corporate vehicles[11] within a corporate structure and so minimize transparency by putting additional layers between the officers and representatives of the company and the ultimate beneficial owners.

IBCs have been available primarily to nonresidents of the United States in offshore locations. The threat posed by these entities is that they are often available off-the-shelf for as little as a few hundred dollars, depending on location, they can be incorporated by using bearer shares or the strategy of nominee shareholders and directors or both, and they may attract little in the way of regulation. Offshore territories that permit the formation of IBCs often have two distinct regulatory regimes, offering greater protection to residents by stipulating that the IBC's products and services can be offered only outside the jurisdiction.

Each of these vehicles or mechanisms is related to beneficial ownership in one way or another, and financial institutions should consider how these risks are to be mitigated. If KYC is the core of AML, then these mechanisms are custom designed to defeat that. The matter is complicated, however, by there being some legitimate reasons for their continued use, related mainly to concerns for personal safety in turbulent jurisdictions and legitimate tax minimization strategies.

AUDITING AND MONEY LAUNDERING

As noted earlier, money laundering is likely to have only a limited effect on the accuracy of financial statements. However, a money-laundering scandal at a financial institution or commercial enterprise can undermine its reputation and put its future in question. The regulated status of a company and the relevant auditing standards of the jurisdiction in which it operates determine the extent to which money laundering gets addressed in the course of a financial statement audit. It is possible that in some of the circumstances discussed earlier, a company committed an illegal act. If this is the case, the various auditing standards governing the auditor's conduct when

[10] Financial Action Task Force, "The Misuse of Corporate Vehicles, Including Trust and Company Service Providers" (October 13, 2006), Chap. 3, § 3.1, Fig. 3.
[11] Organisation for Economic Co-operation and Development, "Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes" (November 2001), 32.

an illegal act either may have occurred or did occur are brought into play. In the United States, for example, a known or suspected incidence of money laundering may require the auditor to extend or expand audit procedures pursuant to Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit,* of the American Institute of Certified Public Accountants, or to report to management and—possibly, in some situations—to the U.S. Securities and Exchange Commission pursuant to the requirements of Section 10A of the Securities Exchange Act of 1934.

Accounting professionals other than external auditors are more likely than external auditors to encounter evidence of money laundering. Financial statement auditors normally test only a small sample of the actual transactions that receive or disburse cash during a fiscal year. Furthermore, money-laundering transactions are normally disguised to look like legitimate business transactions. Internal accountants, by the nature of their day-to-day work and therefore their better knowledge of their business's transactions, are better placed to detect possible signs of money laundering than external auditors. The responsibilities of managers and accountants other than external auditors are addressed in both authoritative and nonauthoritative guidance.[12] Among the varied accountancy roles are the following:

- In-house financial systems consultants
- Internal auditors responsible for operations and compliance auditing
- Practitioners who provide outsourced regulatory examination services
- Forensic accounting investigators
- Public practitioners who perform compliance and operational audits
- Risk management practitioners and compliance specialists
- Tax practitioners, especially in jurisdictions where filings connected with AML laws—such as reports on currency transactions and suspicious activities—are directed to tax authorities

Finally, it is worth noting that in general, internal auditors and other types of accountants who work for management, as opposed to engaging in public practice, are subject to the same AML requirements as the institutions that employ them.

RELATIONSHIP BETWEEN FRAUD INVESTIGATION AND AML

This chapter opened with a discussion of the relationship between fraud and money laundering. Before bringing the chapter to a close, we should briefly consider the similarities between fraud investigation and AML investigation. There are clear

[12] For example, *Anti-Money Laundering,* 2nd ed., an AML discussion paper by the International Federation of Accountants, released in March 2004, web.ifac.org/publications/ifac-policy-position-papers-reports-and-comment-letters/reports-1#anti-money-laundering-2nd. Accountants in management positions whose duties may include recording and reporting entity transactions, such as CEOs, chief operating officers, chief financial officers, chief information officers, controllers, risk managers, compliance officers, and related staff, are more likely to encounter evidence of possible money laundering, as opposed to external auditors performing financial statement audits.

similarities, specifically in regard to the due diligence or research undertaken in relation to companies and individuals. Both fraud investigations and AML assignments are interested in understanding the relationship between individuals and companies. On one hand, in fraud investigations, the search is for an individual or coconspirators, the details of the fraudulent scheme, the scheme's impact on the company, and the control weaknesses that gave the perpetrator or perpetrators their opportunity. AML assignments, on the other hand, often examine customer relationships to verify whether the beneficial owners of financial assets are appropriately identified and reported, and consider whether control weaknesses should be remedied.

Both assignments employ similar techniques, such as data mining, in the course of their investigations. Data-mining software is used in fraud investigations to identify relationships or anomalous transactions within any data under review. Similarly, the technique is used in AML assignments to uncover suspicious transactions, suspicious relationships between accounts, and questionable entities. Viewing both types of assignments from 30,000 feet, one could say that both are concerned with the quality and consistency of the data reviewed.

One of the advantages of sourcing investigative services in the private sector has been that the disclosure of a fraud can often be managed. When a company prefers to keep findings out of the public arena altogether, it may succeed in doing so if it moves quickly and with the right resources. There is, however, still a risk that information may leak to the public and cause both embarrassment and reputational damage. While it may be appropriate to at least begin an investigation before alerting law enforcement, the United States typically requires reporting within 30 days of reaching a conclusion that the activity under review meets one or more of the definitions of suspicious activity.

To return to the points made at the beginning of the chapter, it is conceivable in many circumstances that fraud could be accompanied by money laundering. Whenever there are transactions that move the proceeds of fraud through a business, the activity could be construed as money laundering, particularly when co-conspirators are engaged to facilitate the transaction. The AML responsibilities of accountants vary across the globe. In the United Kingdom, for example, they are covered by the relevant AML legislation. Where AML obligations are extended to cover accounting professionals and forensic investigators, there is an impact on the profession. Where requirements to report suspicion of money laundering are added to AML regimes, the forensic accounting investigator may itself have a duty to report the matter to external authorities. At the same time, if forensic accounting investigators were to become adversarial whistle-blowers, the willingness of regulated entities to engage in self-examination aided by knowledgeable specialists to improve compliance may be substantially curtailed.

As is the case in fraud investigation, AML investigation requires careful and balanced judgments about how to proceed; the input of legal, accounting, and operational experts; and the experience to identify patterns of behavior that are of legitimate concern.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 26

Foreign Corrupt Practices Act

Sulaksh Shah, Dana Weintraub, and Frederic R. Miller

One of the challenges faced by U.S. corporations doing business in emerging markets is dealing with corruption. It is not uncommon for local employees to vent to their U.S. managers about demands from government officials for inappropriate payments and about the competitive disadvantage encountered in complying with the U.S. rules in markets where competitors believe in doing things the local way.

This chapter discusses the background of the Foreign Corrupt Practices Act, recent enforcement trends, the role of the forensic accountant, lessons learned, red flags of corruption, and report writing.

BACKGROUND

The Foreign Corrupt Practices Act (FCPA) was enacted by Congress in 1977 following SEC investigations involving U.S. companies making inappropriate or illegal payments to foreign government officials to secure some type of favorable actions by foreign government officials as well as to expedite routine government duties.

The FCPA[1] was enacted to proscribe bribery of foreign officials. It has three basic provisions.

Antibribery Provision

It is a crime for any U.S. person or company to directly or indirectly pay or promise anything of value to any foreign official to obtain or retain any improper advantage. With respect to the antibribery provision, it is important to note the following:

- A *U.S. person* is defined to include:
  - U.S. citizens, residents, and nationals wherever located (even if the prohibited act did not occur in the United States)
  - Entities organized under U.S. law or entities that have a principal place of business in the United States

[1] Including the 1998 amendments.

  - Issuers of securities in the United States
  - Employees, officers, and directors of U.S. issuers and entities
  - Any persons while located in the United States who act in furtherance of the prohibited conduct
- For example, the SEC settled an enforcement action against Statoil, ASA, a Norwegian company listed on the New York Stock Exchange, for paying bribes to an Iranian government official in return for his influence to assist Statoil in obtaining a contract to develop a significant oil and gas field in Iran and to open doors to additional projects in the Iranian oil and gas industry.[2]
- An indirect payment may include payments to government officials routed through third parties (whether reimbursed or not), including, but not limited, to agents, distributors, joint venture partners, and nominees. For example, in *United States v. Paradigm B.V.*, Paradigm B.V. admitted to the payment of $22,250 into the Latvian bank account of a British West Indies company recommended as a consultant by an official of KazMunaiGas, Kazakhstan's national oil company, to secure a tender for geological software. Paradigm B.V. did not receive any services from the company.[3]
- An indirect payment may include payments to relatives, business associates, favorite charities or funds, and political parties of government officials. For example, in the case of Schering-Plough Corporation, the SEC found that Schering-Plough made payments to a bona fide charity, however, with the intention of influencing the director with respect to the purchase of Schering-Plough's products.[4]
- Until recently, corrupt intent in making payments was generally understood to be a necessary component of an FCPA violation. In a case involving Nature's Sunshine Products, Inc., however, the SEC brought claims against the former CEO and CFO for violations of the books and records provision of the FCPA by holding the executives accountable as "control persons" under Section 20(a) of the Securities Exchange Act of 1934, for failing to adequately supervise the miscreant employees of a subsidiary; the SEC did not allege that the executives had any knowledge of the payments.[5]
- A promise to provide anything of value is tantamount to an actual payment. For example, in *United States v. Frederic Bourke Jr.*, among other things, Mr. Bourke was fined $1 million and sentenced to a year and a day in prison for promising to pay a share of profit realized in a case involving the privatization of the State Oil Company of the Azerbaijan Republic—SOCAR.[6]
- The term *anything of value* is not defined within the FCPA and the regulators interpret it to include cash, gifts, services, travel, business opportunities, tax concessions, and possibly other items. For example, the SEC settled an enforcement action against Bristow Group, Inc., in which Bristow Group allegedly made improper payments to Nigerian state government officials in return for the officials'

[2] www.sec.gov/news/press/2006/2006–174.htm.
[3] www.usdoj.gov/opa/pr/2007/September/07_crm_751.html.
[4] www.sec.gov/litigation/admin/34–49838.htm.
[5] www.sec.gov/litigation/complaints/2009/comp21162.pdf.
[6] www.justice.gov/opa/pr/2009/November/09-crm-1217.html.

reduction of a Bristow affiliate's employment taxes owed to the Nigerian state governments.[7]

- There are exceptions to the antibribery provision for routine nondiscretionary governmental action, such as processing governmental papers like visas and work orders; providing police protection; providing utilities; and scheduling inspections associated with contract performance or the transit of goods across the country. Such payments are referred to as *facilitation payments*. While such facilitation payments are permitted, a U.S. person or company should still comply with local anticorruption laws, which may prohibit such payments as well as complying with the books and records and internal control provisions of the FCPA that are discussed next.

Books and Records Provision[8]

Prepare and maintain books, records, and accounts, which in reasonable detail, accurately reflect the transactions and dispositions of assets. With respect to the books and records provision, it is important to note that *reasonable detail* implies such level of detail that would satisfy prudent officials in the conduct of their affairs.

Internal Control Provision[9]

Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that transactions are recorded appropriately and in accordance with rules and regulations. With respect to the internal control provision, it is important to note the following:

- These internal control requirements are not synonymous with those of Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). Section 404 of SOX requires SEC registrants to establish and maintain an adequate internal control structure and procedures for financial reporting to assist in detecting a material misstatement, whereas the FCPA does not consider the materiality of a transaction. Under the FCPA, transactions must be recorded according to their true nature—gifts to customers must be recorded as gifts, not marketing expense; facilitation payments for customs processing must be recorded as such and not buried in cost of goods sold; and so on, regardless of their size. A company that does not have controls in place over payments that may have FCPA implications will have difficulty justifying the adequacy of their control system on the basis that controls were adequate to prevent material errors in financial reporting.
- Similarly, the internal control requirements of FCPA are not synonymous with the periodic certifications of Section 302 of SOX. Section 302 of SOX requires the principal executive and financial officers of SEC registrants to certify on an annual or quarterly basis, the following:
  - The officers have reviewed the report.

[7] www.sec.gov/news/press/2007/2007–201.htm.
[8] Applicable to SEC registrants only.
[9] Applicable to SEC registrants only.

- The report does not contain any misstatements or omissions of material facts.
- The financial statements and financial information fairly present the financial conditions and results of operations.
- The officers are responsible for establishing and maintaining internal controls, the officers have evaluated the effectiveness of the internal controls within 90 days of the report, and the officers have reported on the effectiveness of the internal controls within the report.
- The officers have disclosed to the auditors and the audit committee any significant deficiencies and material weaknesses in internal controls and any fraud involving management or other employees who have a significant role in internal controls.
- The report includes any significant changes in internal controls or other factors affecting internal controls.

The failure to comply with the internal controls provision of the FCPA may result in inaccurate certifications of Section 302.

RECENT ENFORCEMENT TRENDS

There has been a significant increase over the last several years in the enforcement of the provisions of the FCPA. In 2009, the U.S. Department of Justice and the U.S. Securities and Exchange Commission have brought enforcement proceedings against 46 individuals and 13 companies.[10]

Several trends mark this activity, including: larger penalties, more cases brought against individuals, a larger number of open investigations, a spike in self-reporting of FCPA problems, use of more creative methods in resolution of criminal charges like Non-Prosecution Agreements and Deferred Prosecution Agreements (NPAs and DPAs), post-proceeding imposition of monitors, increased cooperation with foreign and other U.S. regulatory bodies, disgorgement of profits, and increased scrutiny of acts of others.

Larger Penalties

Both the U.S. Department of Justice and the U.S. Securities and Exchange Commission have imposed significant penalties in recent years. As non-U.S. regulators also increase antibribery and anticorruption enforcement actions, many companies are faced with high monetary fines for violations. Some of the most significant penalties imposed are highlighted here.

- *Siemens*—In December 2008, Siemens settled with U.S. regulators for combined penalties of $800 million ($450 million in criminal fines to the DOJ and $350 million in disgorgement to the SEC). This was the largest U.S. monetary sanction ever imposed in an FCPA case at that time. Together with various

[10] PricewaterhouseCoopers analysis and U.S. Department of Justice and U.S. Securities and Exchange Commission web sites.

penalties imposed in Germany, Siemens's penalties are more than $1.6 billion to date. The settlement involved at least 4,200 allegedly corrupt payments totaling approximately $1.4 billion over six years to foreign officials in various countries.[11]

- *Securities and Exchange Commission v. Halliburton Company and KBR, Inc.*—KBR, Inc. and Halliburton Company were both charged by the SEC for bribing Nigerian government officials over a 10-year period to obtain construction contracts valued at $6 billion. KBR and Halliburton have agreed to pay $177 million in disgorgement to settle the SEC's charges. The DOJ also charged Kellogg Brown and Root, LLC, for similar violations and the company has agreed to pay a $402 million fine. The sanctions represent the largest combined settlement ever paid by U.S. companies since the FCPA's inception.[12]
- *BAE Systems PLC*—BAE Systems PLC announced a settlement with both the U.S. DOJ and the U.K. Serious Fraud Office, ending a long ongoing investigation brought by both regulators. Subject to agreement with the court, BAE will pay a U.S. fine of $400 million and a U.K. fine of £30 million.[13]
- *Baker Hughes* settled on April 26, 2007—"BHSI admitted that it violated the FCPA by paying approximately $4.1 million in bribes over approximately a two-year period to an intermediary whom the company understood and believed would transfer all or part of the corrupt payments to an official of Kazakhoil, the state-owned oil company in Kazakhstan." BHSI was subject to the largest combined sanction ever imposed in an FCPA case at the time, facing a $11 million criminal fine, $10 million civil penalties, $23 million disgorgement for $44 million total penalties imposed.[14]

Previous cases with large penalties also include Willbros ($32 million), Chevron ($30 million), and Vetco II ($26 million).

Cases against Individuals

The number of cases and proceedings brought against individuals has increased over the last few years, especially with respect to the activity and reach of the DOJ. As "companies can absorb the cost of big fines and the hit to their reputations . . . the Justice Department is hoping for a bigger deterrent effect by targeting people rather than just punishing their employers."[15]

Mark Mendelsohn, former deputy chief, Fraud Section, Criminal Division, Department of Justice has made such remarks highlighting this trend during his tenure at the DOJ:

---

[11] www.usdoj.gov/opa/pr/2008/December/08-crm-1105.html, www.sec.gov/litigation/litreleases/-2008/lr20829.htm, www.sec.gov/litigation/complaints/2008/comp20829.pdf.

[12] Sources: www.usdoj.gov/opa/pr/2009/February/09-crm-112.html, www.sec.gov/litigation/-complaints/2009/comp20897.pdf, www.sec.gov/litigation/litreleases/2009/lr20897a.htm.

[13] www.baesystems.com/Newsroom/NewsReleases/autoGen_1101517013.html.

[14] U.S. Department of Justice Criminal Press Release 07-296, www.usdoj.gov/opa/pr/2007/-April/07_crm_296.html.

[15] Dionne Searcey, "Currents: To Combat Overseas Bribery, Authorities Make It Personal," *Wall Street Journal,* October 8, 2009.

"If the only sanctions out there are monetary, penalties against companies could be interpreted as the cost of doing business. . . . But when people's liberty is at stake, it resonates in new ways.

"The number of individual prosecutions has risen—and that's not an accident. That is quite intentional on the part of the department. It is our view that to have a credible deterrent effect, people have to go to jail. People have to be prosecuted where appropriate. This is a federal crime. This is not fun and games."[16]

In 2009, 46 individuals were named in SEC and DOJ FCPA enforcement actions. Of those 46, 22 individuals in the military and law enforcement products industry were arrested for "engaging in schemes to bribe foreign government officials to obtain and retain business."[17] There were 16 indictments issued as a result of a sting operation conducted by the FBI and the DOJ, in conjunction with the United Kingdom's City of London Police.

Two other individuals named in a 2009 SEC action were Douglas Faggioli and Craig D. Huff. On July 31, 2009, "The Securities and Exchange Commission filed a settled enforcement against Nature's Sunshine Products, Inc. (NSP), its Chief Executive Officer, Douglas Faggioli, and its former Chief Financial Officer, Craig D. Huff. The complaint alleges that Faggioli and Huff, in their capacities as control persons, violated the books and records and internal controls provisions of the securities laws in connection with improper Brazilian cash payments."[18]

"This appears to be the first time that the SEC has charged an individual under Section 20(a) of the Exchange Act in the FCPA context. The control person theory of liability raises the stakes for officers and directors who are now faced with the prospect of regulatory and law enforcement scrutiny of their leadership, even in situations where they lack knowledge of or involvement in activities several layers of management below them."[19]

Open Investigations and Self-Reporting

At least 120 companies were being investigated for FCPA violations as of 2009.[20] "Over half of FCPA investigations from 2005 to 2008 and roughly half of the open cases in 2008 resulted from voluntary disclosures. One recent case [resulting] from a voluntary disclosure involved Pennsylvania-based transport company Westinghouse Air Brake Technologies Corp. (Wabtec) and its Indian subsidiary, Pioneer Friction Ltd. Following an internal investigation of alleged FCPA violations, Wabtec voluntarily disclosed its finding to the DOJ, which, in February 2008, decided not to prosecute—in return for Wabtec's agreeing to adopt remedial compliance measures. The SEC, however, charged Wabtec with violating books-and-records and internal

[16] PricewaterhouseCoopers, "Corruption Crackdown: How the FCPA Is Changing the Way the World Does Business," July 2009.
[17] http://washingtondc.fbi.gov/dojpressrel/pressrel10/wfo011910.htm.
[18] www.sec.gov/litigation/litreleases/2009/lr21162.htm.
[19] "SEC Flexes FCPA Muscle: Is Change Afoot in the Enforcement Playing Field?" McGuireWoods LLP, *Legal Updates and Articles,* August 25, 2009.
[20] Dionne Searcey, "In Antibribery Law, Some Fear Inadvertent Chill on Business," *Wall Street Journal,* August 6, 2009.

controls provisions, including disgorgement of profits, interest and civil penalties and fined them."[21]

Use of More Creative Methods in Resolution of Criminal Charges (NPA, DPA)

"In many cases, if regulators are satisfied that companies cooperated fully with the investigation and had rigorous FCPA compliance programs in place, then nonprosecution or deferred prosecution agreements may be offered. These agreements may include penalties, disgorgement of profits and the requirement that companies under investigation install a strengthened FCPA compliance program as well as an independent compliance monitor. In 2008, for instance, there were seven deferred prosecution agreements struck."[22]

One such agreement was made with Willbros Group Inc. and its wholly owned subsidiary, Willbros International Inc. The two companies collectively agreed to a $22 million criminal penalty in connection with payments made to Nigerian and Ecuadorian government officials. "In recognition of Willbros' thorough review of the improper payments, the companies' exemplary cooperation, the companies' implementation of enhanced compliance policies and procedures, and the companies' engagement of an independent corporate monitor, the DOJ agreed to defer prosecution of these companies for three years."[23] In a related SEC action, Willbros also agreed to pay $10.3 million in disgorgement and prejudgment interest.[24]

The number of such agreements is likely to ebb and flow over the years depending upon the nature of the individual cases pursued by the DOJ. These methods of resolving cases, however, are likely to remain a useful tool for the foreseeable future.

Imposition of a Monitor

In addition to higher penalties and fines for FCPA violations, regulators have imposed an independent compliance monitor to oversee a company's design and implementation of a compliance program. (See Exhibit 26.1.) The role of the compliance monitor and the duration of this function may vary by company.

In April 2010, the DOJ's settlement with Daimler AG over violations of the FCPA required Daimler to "retain an independent compliance monitor for a three-year period to oversee the company's continued implementation and maintenance of an FCPA compliance program, and to make reports to the company and the Department of Justice."[25] The settlement, which is covered by a deferred prosecution agreement, includes a specific provision outlining the qualifications required by the monitor, the term of responsibility, and the specific requirements and functions of

---

[21] PricewaterhouseCoopers, "Corruption Crackdown: How the FCPA Is Changing the Way the World Does Business," July 2009.
[22] Id.
[23] www.justice.gov/opa/pr/2008/May/08-crm-417.html.
[24] www.sec.gov/litigation/litreleases/2008/lr20571.htm.
[25] www.justice.gov/opa/pr/2010/April/10-crm-360.html.

EXHIBIT 26.1

Case Year	Independent Compliance Monitors
2007	7
2008	6
2009	4
2010*	7 (as of August 2010)

*2010 FCPA data and information were still being compiled as of the time this chapter was written.

the monitor. In the Daimler agreement, such roles and responsibilities include:

- The monitor will review and evaluate the effectiveness of Daimler's internal controls, record keeping, and existing or new financial reporting policies and procedures as they relate to Daimler's compliance with the books and records, internal accounting controls and antibribery provisions of the FCPA, and other applicable anticorruption laws ("the policies and procedures"). This review and evaluation shall include an assessment of the policies and procedures as actually implemented.
- The monitor shall assess whether Daimler's existing policies and procedures are reasonably designed to detect and prevent violations of the FCPA and other applicable anticorruption laws.
- The monitor shall evaluate Daimler's compliance with the agreement.
- The monitor shall oversee Daimler's implementation of and adherence to all existing, modified, or new policies and procedures relating to FCPA compliance.
- The monitor shall ensure that the policies and procedures are appropriately designed to accomplish their goals.[26]

Cooperation with Foreign Regulators and Other U.S. Regulatory Bodies

Many recent U.S. Department of Justice and U.S. Securities and Exchange Commission enforcement releases cite the specific cooperation of foreign regulators and other U.S. regulatory bodies. This reliance on other regulators has increased the country's focus on corruption and bribery. "Regulators are also getting better at ferreting out corruption and are seeing more cooperation with companies and more entrenched collaboration with international counterparts. Increased whistle-blowing, heightened media attention and greater local law enforcement around the world has aided this collaboration. In the past year, for example, the Federal Bureau of Investigation (FBI) has raised its number of agents dedicated to FCPA cases."[27]

In the case of former KBR executive Albert Jackson Stanley, the DOJ specifically acknowledges the "investigative assistance from the FBI and the Internal Revenue

[26] www.justice.gov/criminal/fraud/fcpa/cases/docs/daimlerag-def-agree.pdf.
[27] PricewaterhouseCoopers, "Corruption Crackdown: How the FCPA Is Changing the Way the World Does Business," July 2009.

Service, Criminal Investigative Division. The Criminal Division's Office of International Affairs provided substantial assistance to the DOJ" in gathering evidence abroad and facilitating international cooperation. Significant assistance was provided by the SEC's Division of Enforcement and by the authorities in France, Italy, Switzerland, and the United Kingdom.[28]

Disgorgement

Disgorging profits is a common and prominent feature these days in FCPA settlements with the Securities and Exchange Commission. "Disgorgement of profits in FCPA settlements has risen dramatically, another example of heightening stringency carried out by regulators. In the 2004–2008 period, disgorgement of profits totaled roughly $480 million, with $376 million in 2008 alone."[29] "Prior to the *ABB* case in 2004, the SEC had never collected disgorgement in an FCPA case; since then it has sought it in virtually every case with only a few exceptions, such as *Dow Chemical, Delta and Pine Land, Lucent,* and *Conway*."[30]

The DOJ has also recently exercised its use of disgorgement as well as forfeiture actions against companies, including Chevron. From April 2002 to May 2002, Chevron allegedly made surcharge payments to the Iraqi government in exchange for rights to buy oil, in violation of sanctions and the Oil for Food program rules. Chevron allegedly improperly recorded the payments on its books and records. In November of 2007, the company settled FCPA as well as other violations with both the SEC and the DOJ. Chevron was ordered to disgorge $25 million in profits, and to pay a civil penalty of $3 million. Chevron will satisfy its disgorgement obligation by forfeiting $20 million pursuant to an agreement with the U.S. Attorney's Office for the Southern District of New York and paying disgorgement of $5 million pursuant to an agreement with the Manhattan District Attorney's Office. Chevron will also pay the Office of Foreign Asset Controls of the U.S. Department of Treasury a penalty of $2 million.[31]

Increased Scrutiny over the Acts of Others

Not only are companies responsible for their own actions and activities when it comes to bribery and corruption, but they are now feeling the responsibility for actions that may have occurred within acquired entities or potential targets to be acquired or both. "Increasingly, FCPA compliance is becoming an integral element of pre-deal M&A due diligence. As described in a precedent-setting DOJ opinion procedure release such as 08-02 fully grasping the risks of successor liability has become increasingly embedded as central M&A due diligence tasks. For example, General Electric Company's plans in 2004 to acquire explosives detection systems

---

[28] www.usdoj.gov/opa/pr/2008/September/08-crm-772.html.
[29] PricewaterhouseCoopers, "Corruption Crackdown: How the FCPA Is Changing the Way the World Does Business," July 2009.
[30] "Recent Trends and Patterns in FCPA Enforcement," Shearman and Sterling LLP, March 2009.
[31] www.sec.gov/litigation/litreleases/2007/lr20363.htm.

maker InVision were delayed when General Electric's pre-deal due diligence revealed potential FCPA violations related to payments to foreign officials in China, the Philippines and Thailand. Both General Electric and InVision disclosed this finding to the DOJ and the SEC. Ultimately, the merger was carried out, with InVision paying a penalty and disgorgement of profits."[32]

The SEC has responded to this increased focus on FCPA enforcement actions by creating a new specialized unit dedicated to FCPA enforcement. The Foreign Corrupt Practices Act unit is one of five specialized units. It was established to permit the SEC to be more efficient and less likely to be misled by those who use complexity to conceal their misconduct, and to permit the SEC to be more proactive in deciding on an informed basis where to focus investigations; and will enable the SEC to attack problems systemically, swiftly, and thoroughly and on an industry-wide basis where appropriate. The FCPA unit will specifically focus on new and proactive approaches to identifying violations of the Foreign Corrupt Practices Act. The SEC has observed that in this area, more work needs to be done, including being more proactive in investigations, working more closely with foreign counterparts, and taking a more global approach to these violations.[33]

U.K. BRIBERY ACT 2010

The Bribery Act reforms the criminal law to provide a new, modern, and comprehensive scheme of bribery offenses that will enable courts and prosecutors to respond more effectively to bribery at home or abroad.[34] The U.K. government postponed its implementation to April 2011 to allow for further consultation on how companies can prepare for its demands.

The following is a list of some of the differences between the FCPA and the U.K. Bribery Act in its pre-implementation state:

- Unlike the FCPA, the U.K. Bribery Act covers commercial bribery (in addition to public bribery).
- While the FCPA addresses the person who offers of the bribe, the U.K. Bribery Act addresses the person who offers the bribe as well as recipient of the bribe.
- The U.K. Bribery Act casts a wider web and applies to any entities carrying on business or part of a business in the United Kingdom.
- The U.K. Bribery Act does not permit an exception for facilitation payments or bona fide business expenses directly related to promotional activities.
- The U.K. Bribery Act penalizes corporations for failing to prevent bribery and contains an affirmative defense for having "adequate procedures" in place to prevent bribery.

[32] PricewaterhouseCoopers, "Corruption Crackdown: How the FCPA Is Changing the Way the World Does Business," July 2009.
[33] "Remarks Before the New York City Bar: My First 100 Days as Director of Enforcement," Robert Khuzami, director, Division of Enforcement, U.S. Securities and Exchange Commission, August 5, 2009.
[34] www.justice.gov.uk/publications/bribery-bill.htm.

THE ROLE OF THE FORENSIC ACCOUNTANT

As discussed previously, two of the three provisions of the FCPA deal with accounting-related issues—books and records, and internal control—thereby creating a natural role for forensic accountants in FCPA investigations. Forensic accountants are able to perform a variety of services for clients, including:

- Perform anticorruption risk assessments.
- Design, help implement, and evaluate anticorruption and FCPA compliance programs.
- Conduct transnational forensic investigations.
- Provide enhanced due diligence and business intelligence.
- Design and conduct global anticorruption training.
- Assist independent anticorruption program monitors.

Corruption Risk Assessments

Forensic accountants may be requested by a company or its outside counsel to perform an FCPA risk assessment. The forensic accountant's role may be to conduct the risk assessment or provide assistance to a risk assessment performed by the company's own personnel or its outside counsel. The following procedures should be considered for the risk assessment:

- Gather background information by speaking with key company personnel.
- Understand the type of business the company and its subsidiaries conduct by location.
- Identify the processes and controls within the locations and the type of sales practices used to obtain contracts and business in different locations.
- Assess the scale and volume of business and sales in the various locations.
- Review publicly available information regarding perceived risk and corruption within the locations (Transparency International and other like organizations).
- Gain an understanding of the customers and business practices and business regulations within the locations.
- Assess the use of sales agents and business consultants within the specific locations.
- Understand the various compliance and internal audit functions at the local level.
- Assess controls and policies at the local level with respect to sales and vendor practices and activity within compliance-sensitive accounts.
- Assess the adequacy of controls over bank accounts and disbursements by location.

FCPA Compliance Programs

Based on the risk assessment performed either by the forensic accounting team or the company or both, the forensic accountants may be requested to conduct a

compliance review for specific locations or various business entities and divisions. The review can be limited to one site or country or business unit, depending on the results of the risk assessment and needs and requests of the client. The review may also occur concurrently with the risk assessment, as the forensic accounting team may be requested to join the company's internal audit or outside counsel or both to assist with the risk assessment and identify areas within the company's compliance program to enhance and implement. Procedures to be performed during a review of this type may include the following:

- Speak to key company personnel within the location or business unit.
- Review relevant policies and procedures.
- Identify any departures from policy.
- Assess the compliance and internal audit organizations.
- Review the chart of accounts and receipts and disbursements within compliance-sensitive accounts.
- Gain an understanding of bank accounts and petty cash accounts used and various treasury procedures.
- Perform transaction walk-throughs, as necessary.
- Understand the vendor processes and review vendor disbursement procedures.
- Review various business consultant or third-party sales agent agreements and related disbursements.
- Review contracts and agreements for key projects and key accounts with government entities.
- Review ownership structure and influence with respect to joint venture business relationships and partnerships.
- Report findings and proposed next steps to the company or outside counsel or both.

When reviewing a company's compliance program, the following nine elements may be considered for inclusion within a robust compliance and anticorruption program:

1. Governance accountability
2. Authority and responsibility
3. Disciplinary mechanisms
4. Compliance program standards and procedures
5. Communication and training
6. Policies and procedures
7. Third-party engagement acceptance and retention
8. Monitoring, auditing, and reporting
9. Ongoing improvement

Conduct Transnational Forensic Investigations

From the inception of an FCPA investigation to its completion, various forensic accounting procedures are performed. An FCPA investigation includes many steps to ensure completeness of scope (please refer to other chapters for more in-depth descriptions of the following procedures, as applicable):

Data Preservation and Collection The first step in any investigation is to identify all sources of data relevant to the investigation, which includes, but is not limited to:

- Hard copy documents (including archives)
- Electronic documents, such as scanned documents
- Electronic data, including e-mails, user files, accounting or financial data (including data on shared drives, personal digital assistants, legacy systems, servers, backup tapes, and external media)

Once the relevant sources of data are identified, the next step would be to issue a data preservation notice, which would instruct employees to take immediate steps to ensure that none of the records related to the issue in question are deleted, discarded, destroyed, or modified in any way. The data preservation notice is usually sent by the company's general counsel's office.

Also, since FCPA investigations tend to cross international borders, after considering the implications of local data protection and data privacy laws (discussed in detail in Chapter 9), the relevant data are collected and analyzed, using the tools discussed further on.

Lastly, based on the nature of the allegations and any preliminary findings, it may be prudent to put the employee(s) in question on administrative leave with pay. The advantage of this would be continued cooperation of the employee(s), and an investigation free of any hindrances.

Interviews[35] Interviews form a very integral part of any FCPA investigation and need to be performed during the different phases of an investigation. Interviews conducted during the early phase of an investigation will be informational in nature whereas subsequent interviews may be more specific. It is very important to consider cultural issues during an interview. For example, it is not uncommon in the Middle East for employees to debrief their supervisors on the content of their interview with the investigating team before the supervisor is interviewed. While this may seem unusual to the Western world, an employee's livelihood in the Middle East depends on one's visa or work permit and she is willing to go the extra yard to keep her supervisor happy. In such cases, rather than make an interviewee swear to confidentiality, an alternate approach may be to schedule multiple interviews in a short period and consider doing some interviews concurrently, thus eliminating the window of opportunity for supervisors to be debriefed.

Data Analyses The data analyses would include analyzing financial and nonfinancial data (e-mails, agreements, and so forth). With respect to analyzing financial data, an investigator should consider the following:

Based on the recent enforcement trends and red flags discussed earlier in this chapter, transactions within compliance-sensitive accounts should be analyzed. While it's not possible to give an exhaustive list of such accounts because that

[35] See Chapter 23 for a discussion on "The Art of the Interview."

varies by business and location, some accounts that are commonly considered to be *compliance sensitive* are:

- Donations
- Gifts
- Commissions
- Incentives
- Inspection, licenses, and permits
- Customs and duties
- Consulting expenses
- Legal expenses
- Miscellaneous and sundry expenses
- Entertainment expenses
- Travel expenses
- Training expenses
- Seminars and conferences
- Business promotion expenses
- Facilitation expenses
- Distribution expenses

Also, an investigator should consider using data-mining tools to analyze the financial data in an effective and efficient manner. For example, if the allegations involve a €20,000 kickback to an official in the Department of Agriculture, paid as fees through an intermediary in Florence, Italy, in 2008, the most efficient procedure to identify this and other similar payments may be to perform data mining as outlined here:

- Analyze all payments (focus on cash payments) over a certain threshold (for example, €9,000) recorded in general ledger accounts, including, but not limited to: consulting expenses, professional fees, and legal fees in 2008 and associated with the cost center for Florence, Italy.
- Using wild cards,[36] analyze all searchable fields (for example, journal header, journal description, and so forth) in the general ledger for the name of the consultant as well as the name of the government official in 2008 and associated with the cost center for Florence, Italy.

Based on the results of data mining, transaction testing, interviews, and public record searches, there will likely be a need for additional data-mining procedures.

An integral part of any FCPA investigation is to analyze the nonfinancial data such as e-mails and user files because they are more likely to provide evidence on the intent and culpability of the personnel behind inappropriate transactions. Please refer to Chapter 17 for a detailed discussion.

[36] Wild cards are used to make an electronic search more inclusive. For example, instead of searching for the word *miscellaneous,* it may be more inclusive to use *misc** since it is likely to include *misc.*, as well as *miscellaneous.*

With respect to transaction testing, a detailed discussion on red flags is presented later in this chapter.

Public Record Searches Public record searches are a very common investigative tool in conducting investigations in the Western hemisphere. The amount of information available on publicly available databases is limited in developing countries, however, and as a result traditional public record searches may not be as effective. Since the majority of FCPA investigations involve cross-border issues, it is important to have good tools to perform public record searches to identify information such as:

- Business affiliations
- Market reputation
- Corporate structure
- Locations
- True beneficial ownership
- Government relations
- Prior criminal investigations, convictions, bankruptcies, and so forth

Depending on the country, such public record searches may include:

- English-media databases to determine watch lists, sanctions lists, a "politically exposed person" designation, or adverse information
- Multiple compliance databases
- English-language and relevant foreign-language media database
- Region-specific business or company or regulatory information databases
- Available litigation databases for specific jurisdictions
- Research conducted by trained, experienced, and multilingual due diligence analysts

A cautionary note regarding the use of agents for public records searches is necessary. In many countries, information that is not truly public may be offered by service providers, often with prior experience in governmental organizations or agencies. It is not appropriate to retain such an agent to acquire such nonpublic information, based on their prior working relationships, as payments to existing government employees are often involved. Violating the FCPA while investigating allegations of FCPA violations is not a good idea.

Provide Enhanced Due Diligence and Business Intelligence

Forensic accountants may be requested to assess fraud and corruption risk from a company's use of third-party entities. An assessment of third-party intermediaries can identify facts and information on the entity's reputational, performance, integrity, and business practices, while identifying potential risks associated with new or unknown business partners, agents, joint ventures, vendors, suppliers, and distributors in emerging or expanding market activity.

Design and Conduct Global Anticorruption Training

FCPA and antibribery training may also be provided to a company either as a one-off engagement or as part of a multifaceted FCPA investigation. Training may be presented, along with the company and its counsel and tailored for various audiences, business units, and site locations.

Assist Independent Anticorruption Program Monitoring Agents

A forensic accountant may serve as a designated monitor or independent consultant in carrying out court-ordered or regulator-directed mandates, including the oversight of a company's design and implementation of a compliance program and performance of forensic investigations and assessments.

For more information on the role of a forensic accountant, see also the sections on "The Roles of the Auditor and the Forensic Accounting Investigator," "Teaming with Accounting Investigators," "When and Why to Call In Forensic Accounting Investigators."

RED FLAGS

Anyone conducting business across international borders should consider various areas of vulnerability with respect to foreign corruption. Like many types of fraud and economic crime, corruption may leave behind red flags. Specifically, when performing any FCPA-related engagement, the forensic accounting team may encounter the following examples of red flags.

Cash Payments

Cash is king, especially in developing countries where resident entities do not report all of their income to the tax authorities. The use of cash is so widespread in India that in an effort to detect such practices, Indian regulators require that all cash payments in excess of 20,000 Indian rupees (approximately US$435) be reported annually. As such, any request for payment in cash, especially in excess of certain thresholds, should be scrutinized. For example, in *United States v. Latin Node*,[37] Latin Node entered into sham consulting agreements, providing cash to its employees with which to pay bribes to government officials in Honduras.

Unusually High Commission

It is common for U.S. companies to contract with distributors and agents to increase their overseas market penetration. However, if these agents or distributors, or both,

[37] www.justice.gov/opa/pr/2009/April/09-crm-318.html.

charge commissions that are unusually high when compared to the company's other agents and distributors and to the market, this may be indicative of potential kickbacks or bribes being given by the agents and distributors. For example, in *United States v. Misao Hioki*,[38] Mr. Hioki was found guilty of approving corrupt payments to foreign government officials through local sales agents (as commissions) to secure business.

Consultants

The use of consultants hired without any third-party due diligence as well as a real understanding of the value provided by them could pose a risk of FCPA violations. Because of the intangible nature of services that consultants provide, it is very easy to engage consultants to pay bribes to foreign officials and reimburse them as consulting fees. For example, in *United States v. Siemens*,[39] among other violations, Siemens Venezuela admitted it made and caused to be made corrupt payments of approximately $19 million to various Venezuelan officials, indirectly through purported business consultants, in exchange for favorable business treatment.

Freight Forwarders and Custom Clearing (C&F) Agents

Any U.S. company doing business overseas will typically require the services of C&F agents. However, the following should be considered potential C&F red flags: The invoice includes unsupported sundry or miscellaneous expenses, the invoice includes unsupported round-dollar charges, or the invoice includes the reimbursement of expenses that are outside the contract's terms and are not supported by details or receipts. This last item could be indicative of bribes paid to customs or excise officials. For example, in *United States v. Aibel Group, Ltd.*[40] Aibel Group admitted to conspiring with others to make corrupt payments totaling approximately $2.1 million to Nigerian customs service officials in an effort to induce those officials to give the defendants preferential treatment during the customs process. These corrupt payments were paid through a major international freight forwarding and customs clearance company.

Payments Directed by Third Parties

Any payments requested by third parties to be made to someone other than the third party itself should be viewed skeptically. It is common for officials of state-owned enterprises in many countries to demand kickbacks (which violate the FCPA) that are paid to independent third parties at their request. Similarly, customers who overpay their invoices and then ask for a refund (meant to be a kickback) to be sent at their directions should be processed cautiously.

---

[38] www.usdoj.gov/atr/cases/f240400/240474.htm.
[39] www.usdoj.gov/opa/pr/2008/December/08-crm-1105.html.
[40] www.usdoj.gov/opa/pr/2008/November/08-crm-1041.html.

Overseas Payment Arrangements

Requests or arrangements to pay commissions outside the territory raise several potential red flags. For example, in the course of performing anticorruption and FCPA due diligence on a target Chinese company, a U.S. company identified commission payments made to a U.S. bank account. Upon further investigation, the U.S. company found that these commission payments (for sales orders secured in Latin America) were made to a relative of a Latin American government official who resided in the United States. The company avoided successor FCPA liability by stopping such practices and reduced the purchase price of the business as well.

Delegate Travel

In some countries, especially China, it is common for delegations of officials to visit a U.S. company for a factory inspection. Issues arise when in reality the factory inspection does not occur or takes place on one day and the rest of the trip is spent at tourist destinations such as Orlando and Las Vegas. In *United States v. Lucent Technologies,*[41] Lucent paid more than US$10 million for approximately 1,000 Chinese government officials to take trips to tourist attractions in the United States and around the world. It is important that any delegate travel arrangements are made after due consideration of the business purposes and obtaining the appropriate approvals. In *Opinion Procedure Release 08-03,*[42] the DOJ permitted TRACE International, Inc., to pay certain expenses for approximately 20 journalists employed by state-owned media outlets based in the People's Republic of China (PRC) to enable them to attend a press conference being held by TRACE in Shanghai, because among other reasons, TRACE International, Inc., has no business pending with any PRC government agency, payments do not violate PRC law, and TRACE will accurately record the payments in its own books and records.

Politically Connected Third Parties

Knowing the right people can make a difference, especially in developing countries. While contracting with an established sales agent who is politically connected could definitely have advantages from a business perspective, such a politically connected sales agent may pose a risk of FCPA violation because payments to the agent could be viewed as an indirect benefit to a foreign official as a result of his close relationship or association with the foreign official. For example, in doing business in China, maintaining *guanxi* (relationships) is very important, and a part of maintaining guanxi involves giving gifts, which could have FCPA implications. In the matter of *Schnitzer Steel Industries, Inc.*,[43] to induce government officials in Korea and China to purchase scrap metal, Schnitzer Steel paid them $1.8 million and crossed the line between guanxi and FCPA violations.

[41] www.justice.gov/opa/pr/2007/December/07_crm_1028.html.
[42] www.usdoj.gov/criminal/fraud/fcpa/opinion/2008/0803.html.
[43] www.sec.gov/litigation/admin/2006/34–54606.pdf.

Business in Red Countries

Since 1995, Transparency International, a global civil society organization leading the fight against corruption, has published the Corruption Perceptions Index (CPI).[44] The CPI ranks 180 countries by their perceived levels of corruption and publishes a world heat map. Any company doing business in countries with a CPI of 4.9 or lower (red on the heat map) should recognize the potential exposure and consider the adequacy of their anticorruption and FCPA compliance programs. Similarly, companies operating in countries in which the government participates actively in the private sector or operates utilities or health care and so on, should likewise consider the adequacy of their anticorruption and FCPA compliance programs because of the increase in governmental touch points.

So-Called Facilitation Payments

As discussed earlier in this chapter, the FCPA permits facilitation payments, which by their nature are small and customary in nature. However, just because a payment to a government official is customary or made to expedite services does not make it a facilitation payment. For example, in *SEC v. The Dow Chemical Company,* a fifth-tier foreign subsidiary of the Dow Chemical Company made improper payments to an Indian government official to expedite the registration of three products. The majority of these payments were made through agreements with contractors that added fictitious charges to their bills.[45]

REPORTING

At the start of an FCPA-related engagement, or any engagement, the forensic accountant team should obtain an understanding in advance regarding:

- Whether a written report will be required
- Whether a certified translation of the report is required in the local language
- The degree of formality required
- Who will be the ultimate users of the report (the company, U.S. or foreign regulators, or both). (Please see Chapter 18 for more details on drafting and writing a formal report.)

Views differ on the usefulness of a report on an FCPA engagement. Many clients currently prefer that a formal report not be prepared for various reasons, including potential litigation (third-party shareholder lawsuits) and related issues of privilege. They nevertheless often require that the team prepare a detailed PowerPoint presentation, which is supported by key documents, key e-mails, and transactional support for the findings.

[44] www.transparency.org/policy_research/surveys_indices/cpi.
[45] http://sec.gov/litigation/litreleases/2007/lr20000.htm.

The report, if prepared, and whatever its form, should cover key issues and findings as well as plans for remediation and other next steps. Certain key elements to include in the document should cover the following points:

- What was the alleged conduct?
  - Who participated?
  - Who had knowledge or approved of the conduct?
- Who should have known or would have had oversight?
- Has the alleged conduct been remediated?
- Where did this occur?
- How did this occur?
- What were the preexisting compliance controls in place within this or these countries or business units?
- Is there evidence of other similar behavior elsewhere—how many other countries or business units?
- What are the details on the transactions and problematic payments made?
  - Which contracts or projects or agreements were involved?
  - What is the financial impact of these contracts or projects or agreements?
- Has the company or other parties notified local regulators?

CONCLUSION

FCPA engagements range from the large and complex (with multiple jurisdictions) to small and straightforward. No matter what their size, however, they should be approached with a high degree of experience and professionalism because the potential consequences to client organizations is becoming more and more severe as the international regulatory community redoubles its efforts to root out and prevent corruption. The forensic accountant has an integral role to play in this arena, as many aspects of accounting and accounting record keeping and controls are frequently at the center of any investigation in this sphere, and in fact, two of the three commonly found violations are accounting in nature.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 27

Construction Projects

Daryl Walcroft and Anthony Morgan

Disputes involving construction contracts figure strongly among the assignments offered to the forensic accountant, partly because of the complexity and size of such contracts, in which the amounts disputed often run into millions of dollars. An accountant with knowledge of the construction industry can clarify the issues at the heart of the claim, and his work can sometimes add transparency to the nature and root cause of any cost overruns and assist in bringing the parties together.

What was contractually agreed to will play an important role in determining how a construction claim is formulated or evaluated. While the subject-matter expert should guard against making judgments on legal matters, whether a contract has been complied with or administered correctly or not often depends on the facts of the case, and a forensic accountant may well be able to assist in establishing the facts, particularly when an analysis of electronic and financial data is required.

THE NATURE OF THE CONSTRUCTION INDUSTRY

The construction industry covers a wide spectrum of entities, from the small specialty construction firms to sophisticated multinational engineering, procurement, and construction (EPC) contracting corporations. It is a very competitive industry, where bidding and competing for contracts is routine. It is also an industry where there are relatively low costs of entry for new businesses, so supply often outstrips demand for construction services. In such circumstances, bids have often included virtually no allowance for risk, profit, or contribution to home office overhead costs. The rationale for developing a low bid is threefold. First, even an unprofitable contract provides revenue and work for a workforce during lean times, keeping it together until a better economy returns. Second, it opens the door to work on change orders to the contract resulting from architects' or clients' alterations, or differing site conditions. Change order work can be quite profitable, particularly if more favorable rates than the depressed bid rates can be applied. Third, it can often produce a positive cash flow for a substantial part of the contract, to the benefit of other parts of the contractor's own business. Unfortunately, the practice of obtaining work with below-cost bids and attempting to return a profit on change order work and claims is still prevalent.

A Typical Construction Project

A building contract sounds simple, in theory, when one person formally agrees for payment to carry out building or engineering work for another. In practice, however, problems abound. In the following example, we introduce the players in a typical construction contract and point out some of the common problems that arise.

An employer proposes to construct a new factory on his land. Traditionally, in relation to building (as opposed to infrastructure) contracts, he employs an architect as the contract administrator, who in turn engages a cost professional, a scheduling consultant, a consulting engineer, and possibly other specialists on behalf of the employer. In this example, the architect also acts as project manager. The architect discusses the employer's plans with him and prepares and obtains approval for the detailed plans, which the cost professional will then evaluate to ascertain the quantities of materials and labor effort necessary to complete the factory.

Normally, the cost professional will also advise the employer on the risk allocation in the contract for such matters as responsibility for development of design, plant performance, ground conditions, and also the payment mechanism. The typical alternatives for a payment mechanism are lump sum (fixed price), target cost with incentives, or unit rates (see "Contract Pricing Strategy" further on). The employer then invites contractors to bid on the construction of the factory on the basis of details given by the architect and the cost professional. The contractor normally estimates the cost of the work from the information supplied to him, supplemented by his own inquiries. He also takes into account the time scale for doing the work. The contractor then submits his estimate or bid for the work. Normally, several bidders are invited, to ensure that the work is competitively priced. The contractor will also be aware of any proposed damages for late completion. These late completion damages are known as *liquidated damages* and create incentives for good project management and time management on projects to ensure timely completion.

Next, the employer selects his contractor, normally with assistance from the cost professional. The lowest responsible bidder usually, but not always, wins the contract. A binding contract comes into existence between the contractor and employer when a contractor's bid is accepted.

The contractor may in turn engage subcontractors to assist with performing the work. However, general responsibility for performance and completion of the contract remains with the main contractor. The architect supervises the construction work and normally certifies interim payments against the agreed-upon contract value as stages of the work are completed. The measurement of work done may also involve the cost professional. After evaluation, the employer usually retains amounts (normally up to 5 percent of the cumulative amount paid under the contract) for up to one year after the contract is completed during the warranty period. Alternatively, retainage bonds can be purchased by contractors to allow early release of retainage.

Retention moneys are normally released in two portions: one on the issue of the certificate of substantial completion, and the other on the issue of the final completion certificate. Final completion certificates are normally evidence that the contractor has been paid all moneys due and the building is in compliance with the contract.

On completion, the architect normally issues a completion certificate for the factory building work and determines the final total value of the contract. In this assessment the architect may have to take into account:

- Additional work required and authorized by change orders (due to changes instigated by the client or architect, or for events that were at the owner's risk under the contract)
- Defects in the work of either the main contractor or subcontractors
- Extensions of time for delays to the work caused by the employer (for example, those relating to delivery of free issue materials, lack of access to or the late production of drawings, information, and change orders)
- Delays caused by the contractor (which cause actual completion to be later than the contracted time for performance and could result in liquidated damages)

If the architect and contractor cannot agree on the final value of the contract, it may be referred to the employer, or an initial decision maker (see American Institute of Architects document A201, General Conditions of the Contract for Construction, 2007). If they still cannot agree, the parties must follow a predetermined dispute resolution procedure set out in the contract. Where such a procedure does not exist, they follow statutory procedures. These usually step up incrementally from structured negotiations, to mediation, up to and including binding arbitration or full-scale litigation.

If the factory is completed late as a result of the contractor's default, the employer may consider suing the main contractor for economic loss. To avoid the need to calculate actual damages, most employers include a provision for assessing liquidated damages for a contractor's late completion. Liquidated damages are a fixed daily amount, stipulated in a contract, to be paid by way of damages for failure to complete on time. The amount of the liquidated damages sum should be a genuine preliminary estimate of the loss that would probably arise from a breach of the contract; otherwise, they could be held to be a penalty found to be unenforceable. Liquidated damages clauses do not always deny the employer the right to claim general damages for breach of contract, but this is a specialist legal area of dispute resolution. If there is a dispute over whether the liquidated damages are indeed a genuine preliminary estimate of damage, the expert accountant can often play a useful role in presenting the relevant financial analysis to assist the court's decision on this point.

The contractual relationship must be carefully considered when dealing with legal disputes. In our example, the architect and the cost professional act as agents of the employer and owe him a duty of professional care. The architect is usually responsible for:

- Designing the factory within the employer's indicated price range
- Obtaining a competitive price for the construction work from a competent contractor and subcontractors
- Supervising the construction work in accordance with the designs, price, and timetable
- Reviewing and approving shop drawings, samples, and other submittals made by contractors
- Providing technical answers to questions regarding design as they arise throughout construction

The cost professional is responsible for working from the drawings and information supplied by the architect to quantify the project scope and prepare a quantity take-off, detailing the items and work required to construct the factory, including site clearance, foundations, bricklaying, cladding, painting, and so on. This is a procedure called *taking off*. Contracts normally include an amount for general condition items, such as the erection of temporary site offices for the contractor's staff and architect's representatives, supervision, insurances, supply of site services, site maintenance and housekeeping, and mobilization of equipment. In some contracts, these items are not detailed—instead, rates per hour by grade of worker or job are supplied. The cost professional can be asked by the architect to provide data analysis for assessing claims for moneys due, or claimed, for extensions of time.

The contractor and his subcontractors have to carry out the work in accordance with the contract with the employer. The relationship between the main contractor and his subcontractors must be studied with care, since one or more of the subcontractors may have the same or similar duties as the main contractor.

CONTRACT PRICING STRATEGY

In dealing with construction cases, it is important to know the principal types of contract. While many factors, such as construction techniques and financing arrangements, may have influenced the terms of a contract, management is usually most concerned by the risk factors. In assessing the type of contract to negotiate, the contractor will have carefully estimated the cost of performing the work, the equipment requirements, the timing, the use of subcontractors as opportunities for profit, and the risk element.

The more common types of contract payment terms include:

- Fixed-price or lump-sum contracts
- Cost-plus contracts
- Unit price contracts
- Guaranteed maximum price contracts
- Time and materials contracts
- Turnkey contracts
- Private finance (Design, Build, Finance, Operate; Build, Operate, Turnover; Private Finance Intiative, Public-Private Partnership)

Fixed Price Contracts

Under the traditional fixed price, or lump sum, contract, the entire scope of work is performed for a single price agreed upon in advance. For example, suppose that you arrange for a garage to be built for the price of $25,000. Provided it is completed as required in the contract, with no alterations, the contractor is entitled to $25,000, the agreed-upon price for the work. If the contractor spends $27,000, he is only entitled to payment of $25,000, and will have suffered a loss of $2,000. Fixed price contracts are not generally subject to claims as a result of subsequent fluctuation in costs or quantities to the contract, since the work has been contracted on a fixed price basis, transferring such risks to the contractor. However, if alterations in scope

are imposed upon the contractor, he is entitled to compensation in accordance with the terms of the contract.

Cost-Plus Contracts

Cost-plus contracts have long been favored by contractors and owners when the scope of work has been difficult to define in advance of the work commencing. Cost-plus contracts provide for reimbursement of cost items agreed to in advance, plus a fee for the contractor's services. These contracts are open to abuse by some contractors. For example, when working inefficiently, the work may take considerably longer than planned, justifiably or not, and since the costs tend to increase proportionally with time, the contractor receives a higher fee as a reward for inefficiencies. On the other hand, employers can also abuse mechanisms in these contracts where the definition for *disallowed costs* is open to the employer's interpretation. Cost-plus contracts may be specified as:

- Cost-plus a fixed percentage fee
- Cost-plus a fixed fee
- Cost-plus a fixed fee up to a guaranteed maximum price
- Cost-plus a fixed fee with shared savings incentives

It is important that detailed contemporaneous records for time and materials actually incurred by the contractor are maintained to justify the actual cost of the work. Normally, these contracts require the reasonable endeavors of the contractor to proceed diligently in performing the work, and only costs properly incurred for the benefit of the work are to be reimbursed as actual costs. If the costs are increased because of the contractor's inefficiency, they are likely to be disputed by the employer as *disallowed costs*. The related fee will then be at risk. The costs (both direct and indirect) should be fully defined, so that the employer is protected against waste by, or excesses of, the contractor. The contract terms should carefully specify the reimbursable costs, disallowed costs, the overhead recovery percentages, and the contractor's fee or profit margin.

Unit Price Contracts

Unit price contracts commit the employer and contractor to perform specific tasks at rates agreed upon in advance for a predefined quantity, or unit, of work performed. This could be linear feet of number 8 copper wire, or cubic yards of concrete, or square footage of carpet installed. Normally, the work involved in the project is broken down into quantities (units) and level of effort (hours) in the bid documents for each scope of work. Each contractor bidding for the work submits unit rates, or prices, for each of the listed quantities (unit rates and hourly labor costs). In unit price contracts, the bid documents would normally define the quantities, to allow the bids to be compared on a like-for-like basis. The total of the unit rates multiplied by each quantity (or hour) is referred to as the contract sum. This is not a fixed price, however, as the work is later remeasured on the basis of actual quantities installed, on a monthly basis, and the contract is amended accordingly, subject to any change orders agreed to during the project.

General condition items of general site overhead and time-related expenses are not priced on a unit rate basis, as they are related to the project as a whole, such as insurance, site trailer or vehicle rentals, and mobilization costs. All other costs related to performing the work, however, are deemed to be included in the unit rates.

The contract must specify precisely how each job will be measured. The forensic accountant need not concern herself with the details, as measurement is the responsibility of the project manager, certified cost professional, cost engineer, or superintendent, but she should at least be aware of some of the problems that could arise. Take excavation, for example. The rates for excavation in rock will be different from excavation in soft soil. Furthermore, in both cases the rates may or may not include pumping costs in wet conditions. The rules of measurement can be extremely complicated and involve a considerable amount of professional skill and experience on the part of the engineer and cost professional.

The rates or prices in the bid breakdown will normally form the basis for the architect or engineer to value agreed-upon change orders. There are provisions, even in standard form contracts, however, for change orders to be valued at rates or prices other than those in the unit rates when the latter are inappropriate because of the nature or extent of work affected by the change order. It is not unusual for an owner to include some unit price items within what is otherwise a lump sum contract or other types of contracts.

Guaranteed Maximum Price Contracts

Guaranteed maximum price (GMP) contracts are based on a negotiated estimate, similar to a lump sum bid, but profit is limited to a predefined amount and the actual cost of work is paid incrementally as the work proceeds, up to the value of the prenegotiated GMP. In the event that actual costs are lower than the estimated values, the savings are very often shared with the contractor, on a predefined sliding scale basis. In the event costs are higher, the contractor pays the difference and profit is reduced. GMP contracts can be combined with a target price establishing cost overrun share sliding scales for sharing portions of both cost overruns (up to the GMP) and underruns, below the GMP, with enhanced bonus potential for delivering the project below the target price.

Savings are shared between the owner and the contractor as an incentive to keep the final cost of the project as low as possible. As in a lump sum contract, higher-than-anticipated costs can lead to disputes due to the risk transfer mechanism, and price uncertainty at the outset. GMP contracts are often used in conjunction with *design-build* contracts, through which the contractor is required to complete certain elements of the design on the basis of a set of the owner's requirements or performance specifications. Any changes to the performance specifications or owner's requirements, or differing site conditions, can result in an adjustment to the GMP. Owners are advised to allow for a contingency for any unforeseen cost overruns of this nature, or, in any event, funding sources must be made aware that such increases are possible even with GMP or fixed price contracting mechanisms.

Time and Materials Contracts

Time and materials contracts are similar to cost-plus contracts. Generally, they provide for payment to contractors on the basis of direct labor hours at agreed-upon

fixed rates. These rates are usually composite rates, incorporating amounts for the actual labor cost, overhead, and profit. The costs of materials and other items are specified in the contract. Sometimes, bulk materials for specialized equipment, for example, specialized steel for offshore construction work, may be provided by the employer on a free-issue basis, whereby the employer pays the supplier directly for the material or component and provides it to the contractor to incorporate into the works. The item is therefore free in the context of the contract between the contractor and the employer.

Turnkey Contracts

The phrase *turnkey contract* or *turnkey project* probably originated in the U.S. oil industry. Under these contracts, the project is handed over complete and ready for use: The *key* can be handed over and everything should be ready to operate. The contract may also involve the transfer of technology and the training of the team to run the project after physical completion.

Other expressions, such as *design and build; build, operate, transfer* (BOT); *design, construct, manage, fund;* or *package deal,* have similar connotations. The chief implication is that the employer hands over complete responsibility to the contractor for designing a building or plant to meet the stipulated aims and requirements.

A turnkey contract does not necessarily mean the use of one contract throughout the entire project; the turnkey part may apply only to, say, the camp site, with the rest of the project subject to bills of quantities. The primary advantage claimed for a turnkey contract is that the ultimate costs are lower and more easily controlled. A further advantage often claimed is that construction is quicker under this method. Whether this is really so or not is debatable. A turnkey contract can involve a higher tendering cost and can leave the owner with less control over the project.

Since the contractor is free to innovate within his turnkey contract, the completed structure housing the plant might well be a matter for argument. This is a notorious source for disputes, especially if the performance of the plant does not measure up to the original intention. In this type of contract, in which the employer requests the contractor to design a structure that will do X, Y, and Z, and build it for an agreed-upon price, the employer carries the major risk that the structure will not operate as specified, subject to the financial consequences of performance guarantees provided by the contractor.

Private Finance (DBFO, BOT, PFI, PPP)

A recent form of turnkey contracting has emerged whereby contractors not only bid for the work, but also providing financing, and lease the facility to the owner over a predetermined period, say, 15, 25, or 40 years, for example. This form of contracting is known as a *public-private partnership* (PPP) [also known as *private finance initiative* (PFI); *build, operate, transfer* (BOT); *design, build, finance, operate* (DBFO); and so on]. PPP is a contractual agreement formed between public and private sector partners, allowing increased private sector participation over any other form of contracting. PPP agreements involve government agencies contracting with a consortium of private companies (concessionaires) to renovate, construct, operate, maintain, and manage a facility or system. While the public sector usually retains ownership in the facility or system, the private parties are allowed leniency

in determining how the project or task will be completed and operated. The term *public-private partnership* defines a growing and expansive set of relationships from relatively simple contracts to development agreements that can be very complicated and technical (for example, design-build-finance-operate-maintain). Much of the risk associated with the design and construction of a capital or infrastructure project is usually borne by the municipality or government agency acting as employer in a traditional construction contract. A PPP, however, allows for more of the project risks to be borne by the private sector. The goal of project participants in a PPP framework should be to allocate risk to the party best able to manage it. A key to a successful PPP project is ensuring proper risk allocation is employed, and determining which risks are best carried by the public sector and which risks are better transferred to and managed by the private sector.

STANDARD FORM CONTRACTS

Construction contracts are typically based on industry standard forms of contract. These standard forms have evolved over the years, based on practical experience, and seek to give clarity to the roles and responsibilities of the contracting parties in such a way as to reduce the type of contractual uncertainties that can give rise to subsequent disputes. While many sophisticated and mature clients, contracting agencies, and public authorities have their own customized standard forms, industry-wide forms allow the contracting parties to save time and money having architects or lawyers look over the documents, and permit negotiation to focus on the more practical day-to-day terms such as price and scope of services.

In the past few years, three construction industry associations have revised or reissued their standard contract forms, including:

- The American Institute of Architects (AIA)
- Engineers Joint Contract Documents Committee (EJCDC)
- Associated General Contractors of America (AGC)

The AGC, in conjunction with 19 other construction associations, created a new organization and a new standard form of contract called Consensus DOCS. Other agencies and public bodies that issue standard forms include the Construction Management Association of America (CMAA), Federal Acquisition Regulations (FARs), and Federation Internationale des Ingenieurs Conseils (FIDIC).[1]

The EJCDC contracts have been in use for many years and are favored by engineers who design road and heavy industrial projects. On most large infrastructure projects, however, customized contracts are typically drafted and the terms are negotiated by the parties' lawyers, accountants, and technical advisors. The vast majority of projects in the United States, however, employ the construction contract forms issued by the American Institute of Architects. AIA's principal documents have been designated as *A-series* (owner-contractor), *B-series* (owner-architect), as well as other series. AIA documents are also available as families of specialized editions for use on

[1] International Federation of Consulting Engineers.

different project types. The core family of documents for traditional design-bid-build work use the AIA A-2-1 General Conditions, which includes pricing variations, and abbreviated editions for less complex projects. Many of the AIA forms were revised in late 2007 and contain a number of changes to the documents. All of these standard forms contain dispute resolution clauses.

For example, in the A201 (2007), the parties may select arbitration, litigation, or some other method by means of a checkbox option. If no box is checked, the default process will not be litigated. Further provisions address: procedures for authorizing changes in the work and determining any cost adjustment resulting therefrom; when the contract is to be commenced, whether time is of the essence, the significance of milestone dates, and the availability of liquidated damages for delay; the necessity of protecting persons and property and of insurance; and the termination or suspension of the contract.

If a dispute arises between the parties to a construction contract, new players enter the game. We call these players the *construction litigation team*.

The Construction Litigation Team

Because of the complexity of many construction-related cases, several expert witnesses may be involved (for example, cost, schedule, or engineering experts). Having multiple experts may cause additional problems for the legal teams in coordinating the flow of information among the team members. The experts generally deal with different aspects of the case, but there may well be overlaps, for example, the work of the expert cost professional may have implications for the accountant. Although the accountant cannot demand information from the other experts on his side of the case, he should seek liaison between the professions; there is nothing worse for him than to find himself being contradicted by another expert on his own side. In the end, the legal team will have to determine whether it is necessary for the accountant to be briefed on the other experts' reports. Further complications arise when there are co-defendants, each with their own team of professional advisors. It often makes sense for the accounting expert to act for co-defendants, who will then share the cost of his work, rather than each being supported by their own expert.

As the majority of additional costs arise from delayed completion of a contract (through increased site preliminary costs),[2] claims for delay and disruption and loss of productivity due to a number of changes requested by the client are often put forward by contractors. This leads to a need for an analysis of the schedule to identify the causes of delay and their impact on the contracted completion date.

There are a number of ways that can be adopted to assist in establishing a contractor's entitlement to additional time under the terms of a construction contract. These range from the global, or total time, approach, in which the difference between the total actual duration of the contract and the originally contracted duration is argued to be the additional period of entitlement, to a discrete analysis of each individual cause of delay, how they interact, and their individual impact

[2] Cost-significant items required by the method and particular circumstances under which the work is to be carried out.

to the project's critical path. There are four common methods to choose from, as follows:

1. Affected- or adjusted-as-planned method
2. Windows or watershed analysis
3. Collapsed-as-built method
4. Time-impact analysis

The level of detail that can be applied will be dictated by the quality of the records. Detailed analysis also assists in understanding the amount of overlap that exists between competing delay events. This is known as *concurrency* or *concurrent delay*. Identifying both concurrent delay and the critical path is necessary to establishing which delays actually caused a complex construction project to finish late.

Bar Charts and Critical Path Analysis

To portray the work sequence on a complex construction project, the industry has adopted the use of bar charts and critical path analysis. Bar charts, which are used and understood by site operatives as well as site management, show what construction activities should be happening at particular points in time. Bar charts do not, however, show explicitly how one construction activity, or bar, is interrelated to the other activity bars. It is necessary to understand how construction activities relate to each other for informed decisions to be made about managing them. The most frequently used way of doing this is to link the activities in the bar chart and create an interrelated network of activities that can be analyzed using the critical path method (CPM) of schedule analysis. Once this relationship between activities is established, it is possible to determine which of those activities, if delayed, would cause the project as a whole to be delayed (that is, a critical delay) rather than merely extend the sequence of noncritical activities. Therefore, understanding which activities were critical is fundamental to understanding what caused a project as a whole to be delayed.

The critical path method (CPM) produces a reasonable and reliable objective method for illustrating both the sequence of construction and the complexities involved in identifying and managing interdependent and concurrent activities as well as the delay events affecting them.

To determine what caused a project to be delayed requires a detailed review of what actually happened on the construction project. This analysis should be based on factual records, summarized in the form of a network of activities, which can be analyzed as a whole as well as individually. In this way:

- The starting position is a factual sequence and timing of the construction process (as-built), not merely an estimate of a project's sequence that was not actually followed (as planned).
- The actual labor and equipment records are based on readily supported contemporary information.
- Important delay events are likely to be described in the daily site records.

- The actual overlapping and concurrency of activities can be seen, not just speculated on.
- The actual activities that were critical to completion of the project can be isolated instead of being confused with those generated from a hypothetical plan.

To cover these points in more detail, we next describe different ways of calculating or estimating an extension of time to a contract. The methods we describe can be applied in a number of different ways, which increases the number of variations and permutations possible.

Affected Plan Method

The first method is based on the contract schedule (or a schedule produced at bid stage or soon after commencement of the works). The contract schedule should include both the planned activities and the details of relationships between activities. Extensions of time to the completion date are calculated using assessments of the delays caused by relevant events to the contract schedule using contract documents (that is, the agreed-upon or accepted baseline schedule, method statements, unit rates, bid breakdown, detailed and general specifications, and contract drawings). We refer to the original schedule that existed before any progress or delaying events as the *baseline*. (This baseline schedule, however, could also be the last contractually agreed-upon schedule of work in which, for example, the work sequence has changed significantly or where an acceleration agreement has been made and the project effectively *rebaselined*.)

The extension of time is assessed by adding delays (in accordance with the contract definition of relevant events) to the affected activities in the baseline schedule. The delay assessments are normally based on contemporaneous records (for example, time and material records, or other forced account records). It is necessary for these delay assessments to take into account the effects of mitigating actions taken by the contractor, usually as required by the contract. Once the delays are added to the schedule, it is then possible to compute the revised completion date. The difference between the revised completion date and the contract completion date is the entitlement to an extension of time. The advantages of using the affected plan method are that it is easy to perform, it is cost efficient, and does not rely on the existence of updated schedules. There are several disadvantages of using this method. It does not take into account any inefficiency on the part of the contractor and does not take into account logic or sequence changes, which may cause critical path shifts. Furthermore, the affected plan method is based on a theoretical forecast and does not take into account historical information.

As-Built Method

The second method is very different, as it starts with what actually happened as the basis for determining the extension of time. A network of activities is created on the basis of what actually happened (for example, using progress reports and progressed schedules, diaries, meeting minutes, and other agreed-upon site records). The scope of work (included in the network of activities) may cover the complete works or could be focused on critical work only (that is, those activities that, if delayed, will

delay the entire project). Criticality is determined by calculating the longest route through related activities in the construction process. The delays caused by relevant events are assessed using the same principles as the affected plan method (that is, in accordance with the contract definition of relevant events). These discrete delays are then related to the actual network of activities.

The overall delay to the project can be calculated by consideration of the interactions between activities and the criticality of the activities. This is done by deducting the discrete delays from the actual network of activities, determining the new critical activities, and calculating the date when the works would have been completed had it not been for the delays. The difference between the completion date for the actual network of activities and the calculated date is the extent of the extension of time. A major strength of the as-built method is that it is based on what actually happened on the site. It does not rely on the existence of a schedule. A weakness of the as-built method is that it can be very difficult to identify the true critical path. Another weakness is that it gives rise to the pacing argument. After-the-delay activities are deducted from the critical path, and another path of activities may be of longer duration. As a result, it is hard to determine if the work on this other path was being progressed at a slower pace because of events that were contemporaneously known to be delaying the critical path.

Plan V As-Built Method

The third method of assessing the entitlement to an extension of time compares the as-built schedule to the baseline schedule. This method compares the planned activities from the baseline schedule to the actual schedule. Before the delay can be analyzed, the true critical path must be determined. After the critical path has been determined, the delay is analyzed by looking at each of the planned activities on the critical path and comparing them to the actual completion of those activities. Responsibility for the various delays is assigned to the appropriate parties by careful review of the contemporaneous project records.

This method has several strengths. The Plan V as-built method takes into account what actually happened on the site and compares it to an agreed-upon baseline schedule. This method may be suitable for analyzing projects on which the schedule has not been properly updated. A weakness of the Plan V as-built method is that it does not take into account the dynamic nature of the schedule. The critical path may shift at various stages during the project. As a result, the critical path in the baseline schedule may not be the true critical path at various stages during the project.

Time Impact Analysis

There are two different methods of performing the time impact analysis: It can be performed either during the project prospectively or after the project, using a forensic technique to analyze delay. Performing the time impact analysis during the project requires a periodically updated schedule that reflects both the current as-built data and any logic revisions to the construction sequence. A subnetwork is created when an unanticipated event or change occurs on the project. The subnetwork is inserted into the most current updated schedule and the forecasted impact is analyzed. A time impact analysis performed on an ongoing project is an effective method of resolving

disputes as they occur. The time impact analysis takes into account the dynamic nature of a schedule and the as-built data.

The time impact analysis can also be an effective method of analyzing delay after the project has been completed. Once the project has been completed, actual information is available to analyze the delay rather than the forecasted impact. Using the time impact analysis after the fact also requires a periodically updated schedule. An examination of the schedule updates will reveal the time periods in which the delays occurred. These time periods are referred to as *time windows*. The planned critical path during these time windows must be established from the schedule updates. The as-built dates for the critical path activities must also be established from the schedule updates and the project records for the time windows. The variances between planned and actual critical path performance must be identified. The individual gains and losses in time are summarized to determine the total delay for each time window and the delay is apportioned to the responsible party.

Performing the time impact analysis with historical information has several strengths. The contemporaneous management decisions are taken into account by using the current updates. The dynamic nature of the schedule is also taken into account by using the current updates, and the true impact of the delay is measured using historical information. Also, if the contractor was accelerating the project, that factor is taken into account when the gains and losses are analyzed. The drawbacks to using the time impact analysis with historical information are that it can require extensive data and can be very time consuming.

ISSUES IN ANALYSIS

Some underlying issues in relation to delay analysis methods include:

- The use of critical path analysis to calculate the extension of time and thereby the reliance on:
  - Activity descriptions
  - Activity logic
- The identification of delaying (that is, relevant) events, their impacts, and the party responsible for them
- The use of resources and their efficiency and productivity
- The concurrency of delays (both between and within activities)
- The appropriate level of detail with which the analysis is carried out (for example, taking into account the effects of seasonal working and working time or overtime).

All of these methods usually require full and accurate descriptions for the physical work content represented by each activity modeled. This allows the sequence in which activities are carried out to be accurately represented.

The underlying issues described here are important to the analysis of an extension of time because if they are not handled correctly they can give rise to an exaggerated answer. For example, if delays are assumed to directly affect the completion of an activity, then the contractor's inefficiency in carrying out the work described in that activity might be ignored. The contractor's inefficiency is likely to contribute to the

delay of the completion of the activity and it is not abated when the affected plan method is used.

In summary, any of the methods described may be appropriate for certain applications. Many factors must be taken into account when deciding which method is appropriate for a specific project. A limiting factor when deciding on an appropriate method can be the thoroughness, consistency, and reliability of the project documentation. Creating an as-built schedule requires documentation describing the daily work history that is used for all of the methods described earlier except for the affected plan. Likewise, performing the affected plan and the Plan V as-built methods require the existence of a baseline schedule. The time impact analysis requires a properly updated schedule. All of the methods described earlier have their inherent strengths and weaknesses. These strengths and weaknesses must be considered when deciding on an appropriate method to analyze delay.

No matter which of the foregoing methods is selected, it is likely that the usual issues that arise on consideration of extension-of-time claims will have to be evaluated by the forensic accountant. The usual issues relate to:

- Concurrency of delay between the parties
- The critical path in the schedule of work
- The ownership of float when early completion is anticipated
- A lack of evidence on the loss of productivity
- What, if any, steps the contractor took to reduce or mitigate the impact of delay to completion, for example, through resequencing parts of the works, working weekends, or longer shifts

All of the standard forms of contract listed earlier provide a mechanism for dealing with and evaluating claims arising in the course of performance-of-construction contracts. These claims may be for additional costs arising from change orders to the contract, for example, through changes in design or methods of construction. They may be for direct loss or expense arising, for example, from delays or rescheduling of work. We describe these two types of claims next. Provided the contractor follows the procedures for making a claim, she has a means within the contract for resolving disputes. The fact that certain claims may be quantified by reference to the contract does not prevent a contractor from seeking damages under common law rights for breach of contract.

CHANGE ORDERS

Change orders to the contract are generally valued by the appointed cost professional. When the bid breakdown contains rates for the compensation of material, labor, and so on, involved in the change order, these are usually used for valuing the amount of the change order. When the work is of a similar nature, the unit rates are used, subject to an appropriate allowance for difference in conditions, height of working platform, or access, if any. If the bid breakdown provides no suitable yardstick, the items comprising the change order are often negotiated using fair rates and prices, or preferably, actual cost based on receipts, signed work tickets, time sheets, and invoices.

To determine fair rates or prices, the cost professional normally takes account of the prices contained in the original bid breakdown. If the contract was priced competitively or at a loss, then similar pricing, using tendered resource costs and productivity, will be applied to change orders.

When change orders cannot be measured reasonably, valuation on a *day-work,* or time-and-material, basis may be used. In essence, day-work rates means either a schedule of rates that may be based on a working rate agreement or actual cost plus a percentage—such percentage being established as an industry norm—to cover overhead and profit. The norm can change over time, reflecting the extent of competition in the industry.

A *quantum meruit* valuation—that is, one based not on the terms of a contract but on how much is deserved for work done—is not normally used by the architect or cost professional unless the contract authorizes him to do so.

Because bill rates are the prime source for valuing change orders, errors or inconsistencies in the rates appearing in the bid breakdown can give rise to difficulty if they come to be applied for change orders. For this reason, a bill is generally scrutinized for such errors before the contract is signed. Where such errors are discovered in lump sum contracts, it is often the case that the contractor is asked whether she wishes to stand by her rates. If not, the rate and pricing can be corrected. However, because the individual items will now not add up to the lump sum, a percentage adjustment is applied to all the items on the bill to compensate for the error, so that the amended bill still adds up to the original lump sum bid price.

When, later, the bill is used to price change orders, the cost professional must ensure that any percentage adjustment to the rates is taken into account.

Provisional Sums

Sometimes an employer puts a contract out for bid before he or the architect has decided on the detailed specification of some part of the building. In these circumstances, a general description for the works is given, and the architect or cost professional puts in a provisional sum for the work. Although these are estimates, they are based on what is considered likely to be expended.

When the work has been completed and the work valued, the provisional sum is replaced by the actual value of work carried out. This may be valued at the actual price or in such a way as the contract specifies.

FINANCIAL DAMAGES

Standard form contracts commonly allow for claims to be made if contractors suffer direct financial loss as a result of an event that entitles the contractor to a change order. If the amount of a change order cannot be agreed to through negotiations, contractors will be forced to prove their level of damages actually experienced with a reasonable degree of accuracy. If the damages are caused by a breach of contract by one party or the other, the courts will generally try to put the claimant back into the financial position it was in before the breach occurred. This is true in tort or breach of contract. Contract damages are generally compensatory in nature, meaning they

provide claimants the ability to recover both losses caused as well as gains prevented. Damages can be made up of either direct costs or indirect costs.

Direct costs are those related to the immediate impact of the event (labor, material, equipment, extended time-related performance costs, and so on). Consequential damages are the indirect source of loss as a result of the breach. Consequential damages need to have been reasonably foreseeable by the parties when they entered into the contract. This definition flows from case law, and particularly the rule in *Hadley v. Baxendale* (1854) Eng. Rep. 145, which is widely relied upon and accepted by U.S. courts.

To succeed in recovering damages in construction claims, the claimant must prove entitlement (liability on the other party), and establish a cause-and-effect nexus from that event to financial loss and the level of damages actually caused by the event. In practice, claims on construction contracts often involve a number of interrelated events whose effects on time or money are often difficult or impossible to ascertain discretely. In such circumstances, the courts may not require the losses caused by each separate event to be separately identified, and the claimant may adopt a total-cost approach when quantifying damages. A total cost calculation is simply a comparison of a contractor's actual costs, plus a reasonable overhead and profit margin, to the amount of actual payment received. By subtracting the payments received from the cost incurred, the difference is claimed, as if the contractor were fault-free and the defendant was 100 percent responsible for all cost overruns. This approach is clearly preferred by contractors. For obvious reasons, it is discouraged by the courts. To pursue a total-cost claim successfully, the courts have established an arduous set of hurdles for a claimant [see *Blinderman Constr. Co. v. United States,* 695 F. 2d 552, 559 (Fed. Cir. 1982)], including:

- Any other method of calculating damages on a discrete basis is impossible or commercially impractical.
- The actual costs incurred must be reasonable.
- The contractor's bid must be shown to have been accurate.
- The actions of the plaintiff must not have caused any of the cost overruns.

A generally accepted method of applying the total cost claim can be achieved when claimants make appropriate reductions to their actual costs, allowing for the cost of events that were not the liability of the defending party. This approach is known as a *modified total cost* claim and is generally more accepted by the courts. The courts applied this four-part test for recovery under the modified total cost method articulated in *Servidone Construction Corporation v. United States,* 931 F. 2d 860, 861 (Fed. Cir. 1991) and Boyajian, supra, 423 F. 2d at 1243. They tested: (1) the impracticality of proving actual losses directly, (2) the reasonableness of its bid, (3) the reasonableness of its actual costs, and (4) the alleged lack of responsibility for the added costs.

The modified total cost method is the total cost method with adjustments for any deficiencies in plaintiff's proof in satisfying the four requirements. The modified approach assumes the elements of a total cost claim have been established, but permits the court to modify the test so that the amount plaintiff would have received under the total cost method is only the starting point from which the court will adjust the amount downward to reflect the plaintiff's inability to satisfy the test.

The court found that the claimant in this case failed to demonstrate the first element of this four-part test because the plaintiff failed to prove that it sustained damages that could not be ascertained and measured with reasonable certainty.

If the expert is engaged in respect of either delay or cost by a contractor making a global claim, she should expect to be asked to state and show in her report what she has done to try to carry out the exercise of showing causal linkage.

Typical heads of a construction contract claim for direct loss or expense or both are:

- Onsite establishment costs
- General or head office overhead
- Loss of profit
- Increased cost of working
- Financing charges and interest

It is established as a matter of principle that claims for appropriate head office costs are allowable as part of a claim for direct loss or expense or both.

The calculations of loss of profits are therefore relevant to these claims. The claimant is entitled to recover the difference between what it would have cost but for the delay and what it actually cost. The rates used in the bills of quantities are generally irrelevant for this purpose. A number of features of these claims merit specific comment here.

Overheads

A claim for overhead is a difficult one to make, but it must be tackled in any review of a contract dispute. Some contractors divide their overhead between preliminary items and bid breakdown items, without giving precise indications of what they have done. As a result, when a major change goes to the heart of the contractual price arrangements, the contractor may claim that the unit rates in the bid breakdown are inadequate. For example, if less work is done than was foreseen in the original bid breakdown, he might claim that he has failed to recover his offsite and onsite overheads in full. Alternatively, if he has done more work than was contemplated in the bid breakdown, he may claim additional overheads on the grounds that the levels of supervision and skill required in the offsite and onsite offices were so great that the overheads went well over the sums he had expected when he submitted his bid. These are fertile areas for dispute, and accountants are well placed to advise on the solution. Ideally, the accountant should, if possible, examine the total overheads incurred, period by period and category by category. Remember, the purpose of the claim is to put the claimant back in the position he would have been in but for the event being complained about.

On occasion, claims are evaluated by reference to bid rates, including provisions for subcontract costs. Care must be taken that the amounts claimed represent genuine costs. It is therefore necessary to determine how much has (or is likely to have) actually been paid to subcontractors, after taking into account any claims and counterclaims. It is also necessary to investigate any recoveries that have been made by way of insurance claims. A related subject that needs careful handling is the extent to which losses arising out of any event have already been reimbursed by way of

a claim against the main contractor. Since there is a tendency for a settlement to be made on a lump sum basis, this subject can give rise to significant differences of opinion upon which the accountant can often shed helpful light.

At an early stage in her work, the expert accountant will have to consider what jurisdiction is relevant. Many large construction contracts are carried out abroad. A claim may have to be quantified on different bases, depending on which jurisdiction is relevant. It is up to the accountant expert to be aware of the various possible routes toward quantification of a claim. Before she commences on her report, the proper basis should be agreed upon with the legal experts.

Since overheads tend to be fixed in the short-to-medium term, a change order to the contract or a delay does not necessarily affect the offsite costs. Nevertheless, in the contracting industry such overhead costs have to be paid for out of work done. The costs are generally a function of time, although method-related overheads do also occur, for example, when, due to delay, a concrete batching plant has to be decommissioned and then remobilized. If delay occurs, these costs continue without any contract income to cover them. They are often described as unabsorbed overheads. In many cases, it is appropriate for this loss to be included in the claim. A word of warning, however: The contractor may have a number of contracts or claims in progress that are all contributing to overheads. The accountant, therefore, needs to assess whether a further claim for overheads will represent an excess recovery. Similarly, if other parts of the bid breakdown make allowance for local office overheads—for example, in the onsite costs—double counting may occur.

Contractors frequently price bills of quantities at rates that cover preliminary and offsite overhead costs. As a result, when there are substantial change orders that are priced at these rates, the contractor receives, through change orders, a contribution to his on- and offsite overheads. Substantial change orders often cause delay in the general progress of the works. Claims for change orders, therefore, tend to go hand in hand with loss and expense claims for delay. If the expert accountant is retained to assess the loss and expense claim, he should take care that there is no duplication of this claim within the measured change orders in the final account.

In our experience, the contractor sometimes objects to the disclosure of project costs to an investigating accountant. In a dispute, such objections should not be sustained if the contractor is alleging that there has been a fundamental change in her expectations on overhead costs. As a rule, if a major extension has been made to the contract, the contractor should be willing to reveal all project costs.

Skepticism arises if the contractor says that a major increase in the scope of the project will add to the unit cost of overheads, when there is no change in the nature of the overheads required to service the change of scope and the time period is the same. After all, common sense says that spreading the overheads over a greater amount of direct output produces some economy of scale. The contractor may have left out altogether the overhead contribution when pricing the job (perhaps because he was short of orders). A major extension in the scale of the work will then clearly hit him hard, particularly if the extra work prevents him from taking on other, more remunerative, work.

If, on the other hand, he has had to do much less work than that allowed for in the bid breakdown, the contractor may not be able to recover the overheads built into his costs. Whether his claim is realistic or not will depend on the circumstances;

if the time needed to do the job has decreased, he may be able to fill the remainder of the time with other work, thereby mitigating his loss completely.

Computing the amount of overheads to allow in a claim is fraught with difficulty. The industry and the courts have endeavored from time to time to establish formulas for deriving the amounts, for example, by computing contract overtime costs per day or per $1 of direct cost. There is inevitably a trade-off between simplicity and fairness. The important decision is to choose the most appropriate approach for the individual claim. It is important also to recognize the circumstances in which a court is willing to embrace the use of formulas.

It was held in *Norwest Holst v. CWS* (1998) (unreported) that an appropriate formula may be used in the following circumstances:

- The loss in question must be proved to have occurred.
- The delay must be shown to have caused the contractor to decline to take on other work that was available and would have contributed to its overhead recovery. Alternatively, the delay must have caused a reduction in the overhead recovery in the relevant financial year, which would have been earned but for that delay.
- The delay must not already have had associated with it an increase in recovery or contribution toward overheads, for example, through an increase in contract value by change orders.
- The overheads must have been incurred in any event without the contractor achieving turnover to pay for them.
- There must have been no change in the market affecting the possibility of earning profit elsewhere, and an alternative market must have been available. Furthermore, there must have been no opportunity for the contractor to deploy its resources elsewhere, despite the delay; that is, there must not have been a constraint in recovery of overheads elsewhere.

There is a clear role for the financial expert here in helping to establish whether alternative work was available upon which the contractor could have used his resources, but for the delay.

Loss of Profit

Although many contracts explicitly do not allow claims for profit, a contractor may be entitled to claim for loss of profit if she can demonstrate that she would have earned that profit but for the delays, disruption, changes, or whatever she is complaining about. She has to show that, where there is disruption or delay, she has been prevented from earning a profit elsewhere in the normal course of business. That is to say, because her resources have been tied up on a delayed contract, she has not been able to take up other contracts.

Faced with this sort of claim, we find it helpful to analyze the contractor's general level of profitability, looking, for example, at her general business performance as disclosed by audited accounts or the profitability of a range of recent similar contracts.

We also examine whether the market at the time was active or slack. Sometimes a contractor computes a claim for loss of profit based on the profit percentage she

builds into bids. This can be misleading. There can be a considerable difference between expected and actual profit, and careful attention should be given to this aspect of a claim.

Increased Cost of Working

Although, clearly, performance on the contract in dispute is of primary importance, faced with a claim for increased cost of working, we find it helpful to analyze the contractor's general level of profitability and throughput. For example, we may look at his general business performance as disclosed by audited accounts or the profitability of a range of recent similar contracts, and compare planned and actual production as shown on the management production schedules. Amounts claimed in respect of alleged idle time should be restricted to loss of profits and overhead recoveries that could have been achieved on other profitable work that it is reasonable to believe would have been carried out in the absence of breach.

Equipment hire rates are often an issue in cases of idle time, although in many instances equipment is hired for a fixed period. Provided the delay does not result in the hire period being extended, there is no loss. Where the equipment is owned, it may also be appropriate to relate the loss to a hire rate; some adjustment will be necessary to eliminate the profit and overhead contribution built into the hire rates. Alternatively, the loss may be reflected by a depreciation charge. In this case, we expect to see a lower-than-normal rate applied since idle equipment tends to depreciate more slowly than active equipment. Maintenance costs may also be relevant, but their impact will depend on whether idle equipment needs more or less maintenance than the working equipment.

It is important to identify the specific factors causing the delay and whether these were the fault of the employer or the contractor. It must also be ascertained whether these delays affected the critical path of the contract schedule. (The critical path is the longest sequence of steps in the construction schedule.) It should be noted that the critical paths can change and that there can be more than one critical path.

Increased costs often arise in cases of delay and disruption because of inflation and the effort needed (for example, overtime working, inefficient working) to restore the project to its original timetable. Such claims should be accounted for in detail and relate cause to effect.

Finance Charges and Interest

Under the concept of direct loss or expense (or both) in the JCT forms, finance charges, and in particular interest on money expended, are allowable as a head of claim, as is loss of interest on money diverted from interest-earning investments. However, simply applying a reasonable commercial rate of interest to the losses under other heads of damage is not enough. The claimant must produce supporting evidence to demonstrate the loss, for example, proof that overdraft interest was incurred.

Furthermore, it has been established that the contractor has an obligation to continually update the employer with the accrual of finance charges. There is, of course, a general need for the contractor to keep contemporary records of extra expenses incurred and their causes if, at a later date, disputes have to be negotiated or settled.

UNDERBID

We have already stated that some construction industry contractors deliberately underbid, either because they are desperate for work or because they hope, by careful claims creation later, to make good any price shortfall in the original quotation. We have also said that, if an item was priced at a loss, that price should also apply to change orders if the bid conditions existed at the time of the change order.

It may be useful, with the assistance of the employer's engineering advisors, to assess the extent to which the contractor has underbid when quoting for a contract. No precision can be claimed for such exercises, especially if the employer (the defendant, in this example) has not seen the details of the claimant's original bid. Even then, however, clear clues may demonstrate an underbid.

If the contractor (or a subcontractor) has underbid by a factor of, say, two or three, disaster will follow. She may be able to legally prove that she was misled as to the work required, the difficulty of the design, or, for example, the quality of the rock that had to be excavated. But to support her assertions, she will have to show that there was good reason for her bid price to be, say, half of the next lowest price.

The accountant must get down to the basics behind the contractor's estimate. This will often involve taking a view of the number of labor hours required for a particular part of the contract, or perhaps of the weight of metal required, in addition to the question of overheads.

A clear indication of an underbid by a subcontractor may arise when the general contractor has priced some work that he is undertaking that is the same, or very similar to, work subcontracted to someone else. If the general contractor's assessment of the cost is, say, twice that of a subcontractor, the latter is putting himself in peril and should not look to later claims for change orders or disruption to recover from his initial error.

In short, the courts will not feel inclined to let a contractor off the hook if she has underbid or been careless, or has simply failed to appreciate the risks she is undertaking.

INFLATION

Increased costs can often be the subject of a claim where there has been significant inflation since the contract was signed. The investigating accountant should beware of a claim for generalized increased costs—particularly for unit prices—showing standard increases in all costs over some period of time. Costs fluctuate, and the relationship between the costs in a claim for different periods may not be linear. Price indexes and statistics, widely available from libraries and government departments, should be reviewed to determine whether the trend claimed is in line with costs in the country as a whole. Care must be taken to ensure that the country index chosen is relevant, bearing in mind the source of the materials or equipment concerned.

ANALYSIS OF CLAIMS

The variety of problems found in construction claims is considerable; in the following tables, we have broadly divided the causes between those arising from change order,

EXHIBIT 27.1 Change Orders to Contract

Effect on Claim	*Areas for Inquiry by the Accountant*
Increase in preliminaries	Was genuine additional expenditure incurred?
Changes to materials used—both volume and type	Are unit rates valid? Were materials necessary?
Change in labor mix	Were genuine additional costs necessarily incurred or did the work absorb idle labor?
Additional labor hours	Are the rates applied appropriate?
Change in equipment and machinery usage	What was the real cost of the equipment usage?
Allowance for overheads and profit	Were any additional overheads incurred? Was there loss of opportunity to carry out other profitable work?
Allowance for financing costs	Was the company a net borrower of funds, and if so, at what rate did it borrow?
Additional costs arising through acceleration of work	Were the additional costs directly attributable to the acceleration of work or do they reflect inefficiency by the contractor?

those from delay, and those from disputes as to original specification. (Disputes as to original specification are distinct from change order disputes in that they go to the heart of what information the contractor was given originally when he was requested to bid.) We then describe the effect that these basic causes can have on direct loss or expenses (or both) and suggest areas of inquiry for the accountant to follow through with. (See Exhibits 27.1 to 27.3.)

EXHIBIT 27.2 Delay

Effect on Claim	*Areas for Inquiry by the Accountant*
Increase in preliminaries	What additional charges were actually incurred?
Idle direct labor	Could labor have been redeployed or laid off?
Idle equipment and machinery	Was there any alternative use for equipment and machinery?
Additional overhead costs	Were there any genuine increases in indirect costs or overhead expenditure?
Demobilization and remobilization costs	Were these costs genuinely increased, for example, to mitigate loss?
Extra remedial costs and costs of making good after delay	Did the delay cause deterioration to the works that had to be made good before completion?
Escalation to unit rates on productive work	What increase in underlying cost rates affected the project?
Loss of profit	Did the delay give rise to loss of profit opportunity elsewhere?
Additional financing charges	Was the company a net borrower of funds, and if so, at what rate did it borrow?

EXHIBIT 27.3 Disputes Concerning Original Specification

Effect on Claim	*Areas for Inquiry by the Accountant*
Increase in preliminaries	Was proper cognizance taken of preliminaries in the original bid?
Additional materials	If genuine, were they acquired at best rates?
Change in labor usage and mix	Are rates for different labor grades appropriate?
Additional wear and tear on equipment and machinery	What rates of depreciation are applied to equipment—were any fully written off?
Additional overheads	Was the original overhead recovery rate appropriate? Has the change in specification affected indirect costs in any way?

SUMMARY

In looking at claims for construction costs, it is initially desirable to assess their overall reasonableness by some broad tests: The costs of the principal components of most contracts tend to conform to a similar pattern. For example, the costs of design and supervision and project management seem to bear a direct relationship to the value of the contracting work performed. Experience has shown that design and supervision costs usually represent some 10 to 15 percent of total construction costs; project management costs tend to represent 1 to 3 percent of the total. Contract overheads range as follows:

- Site overhead: 3 to 10 percent
- Head office overhead: 5 to 10 percent
- Engineering and supervision: 7 to 21 percent

These guidelines should not be considered definitive, as they do tend to change from time to time, reflecting market and competitive conditions, but they may help the expert accountant consider the overall reasonableness of a claim and to direct her work toward those areas where the claim appears unduly heavy.

Finally, thought should be given to the pros and cons of settlement versus continued dispute. Almost always, there are commercial considerations to be taken into account. What is the potential prize? What is the cost of winning it, and what are the chances of success? Construction claims, whether heard by the courts or in arbitration, tend to lead to lengthy trials. We know of one case that was expected to last nine months to a year. When the experts' reports on quantum were exchanged a few days before trial, it became clear that the quantum gap between the parties was so small that it made the litigation uneconomic. The case was settled. If the quantification of damage had been given a higher priority in preparation for litigation, much expense could have been saved.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 28

Contract Compliance

Jeff Leedom, Philip Treccagnoli, and David L. Marston

Large complex contracts are a significant part of today's global business environment. Most companies negotiate both large and small contracts with a goal to drive business value. In fact, in some businesses, large contracts are the foundation for significant international corporate relationships as well as the overall value of the companies involved.

Despite the importance of contracts, they are not all created equal, and furthermore, not all contracts are complied with by each and every business partner. In fact, contract compliance, or should we say noncompliance, is a significant issue that plagues organizations throughout the world without bias as to industry, geography, or company size. Also, contract noncompliance is an issue that covers a broad range of business contracts and can have lasting impact. Some of the types of contracts that are frequently affected by noncompliant behavior include, but are not limited, to the following:

- Licensing
- Sourcing
- Co-development
- Distribution
- Service
- Advertising
- Franchising
- Joint ventures and partnerships
- Government procurement

The failure to comply with contractual terms can arise from many different types of contracts, and the type of noncompliance can come in many forms. The following are a few examples of how business partners fail to comply with contracts:

- Lack of appropriate controls over the reporting process
- Mathematical and clerical errors
- Failure to apply basic contract terms
- Ambiguous and unclear wording in agreements
- Failure to dedicate appropriate resources and oversight to the royalty reporting function

- Lack of communication or coordination among various departments
- Lack of understanding of contractual obligations
- Turnover in key personnel
- Intentional noncompliance and fraud

Contract compliance is an issue that can have extreme negative effects on an organization if business partners fail to comply with these types of contracts. In fact, in many cases a business partner's noncompliance can cause significant revenue leakage or increases in costs. Whether the noncompliance causes lost licensing revenue, an increase in material costs, or even an inequitable share in co-development costs, one common theme is that noncompliance is pervasive throughout the population of contracts listed earlier. In fact, the overall negative economic impact caused by noncompliance is as high as several billion dollars each year. Accordingly, forensic accountants are frequently called upon to assess the facts and circumstances surrounding one or more parties' compliance with contractual terms.

Even though the economic impact can be severe, many companies are not proactive and do not take the necessary steps to mitigate contract compliance risk. There are many things that companies can do to recuperate past loss as well as minimize future risk arising from noncompliance. The following is a discussion of many of the steps that companies can take, with a separate section discussing some of the unique challenges presented by government contracts, and the role that the forensic accountant can play to assist companies and governments with this goal.

EFFECTIVE INTEGRATED INTERNAL AND EXTERNAL CONTRACT COMPLIANCE PROGRAM

There are many steps that companies can take to implement a contract compliance program that improves the relationship with business partners as well as mitigates the contract compliance risk that they face. The processes, controls, and policies that are employed to manage an internal contract compliance program can be as important as the efforts that are made from an external perspective. In general, a successful internal compliance program has processes and controls that help do the following:

- Effectively manage internal communications between compliance officers, legal personnel, accounting and finance, and sales and marketing individuals to leverage all necessary information.
- Create clear lines of communication between business partners to build transparency and trust.
- Effectively organize and store relevant documentation important to monitor and manage business partner relationships.
- Perform data analytics around market intelligence and business partner reporting.

Both the internal compliance program and external compliance efforts should work together as an integrated system to provide valuable feedback, intelligence, and information to maximize the effectiveness of the overall compliance program. See Exhibit 28.1.

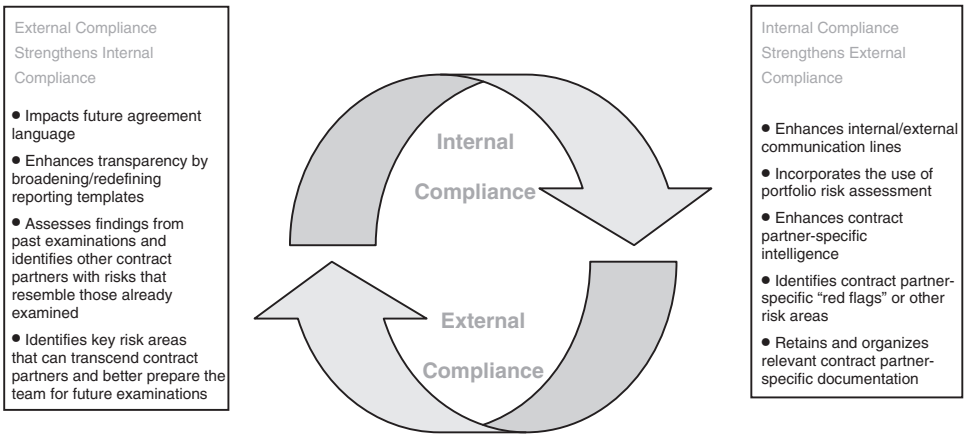


EXHIBIT 28.1 Contract Compliance Program Feedback Loop

Therefore, if the appropriate compliance program controls are employed, both the internal and external programs can provide valuable feedback that improves the overall effectiveness of a company's contact compliance efforts.

Contract Portfolio Risk Assessment

It is important to understand the impact that due diligence and an effective contract portfolio risk assessment can have on the overall success of a contract compliance program. A comprehensive approach to a portfolio risk assessment enables companies to effectively analyze a specific contract partner's potential compliance risks, make educated compliance program decisions, and enhance the value of compliance examinations and overall contract compliance program results.

The risk assessment starts through careful identification of risk factors, stratification of the contract portfolio, and calculation of an actual risk score for each contract. The output from this risk score can be used to make critical contract compliance program decisions. A simplified example of the output from this tool is illustrated as follows.

Both qualitative (for example, location of counterparty, reputation, past experience with party, difficulty, timing, significance to operations, level of detail provided in reports, apportionment concerns, organization complexities, third-party involvement) and quantitative (for example, fluctuation in profit margin, size, loss exposure, number of units, duration, complexity of calculation) factors should be considered when determining the overall risk of a contract partner. Exhibit 28.2 depicts the use of both of these categories of risk as well as the current financial impact that each contract partner contributes to the portfolio (indicated by the size of each of the circles).

Consistent Business Partner Communication

Many business partners' failure to comply with contracts can be mitigated through simply keeping consistent and effective communication open between business

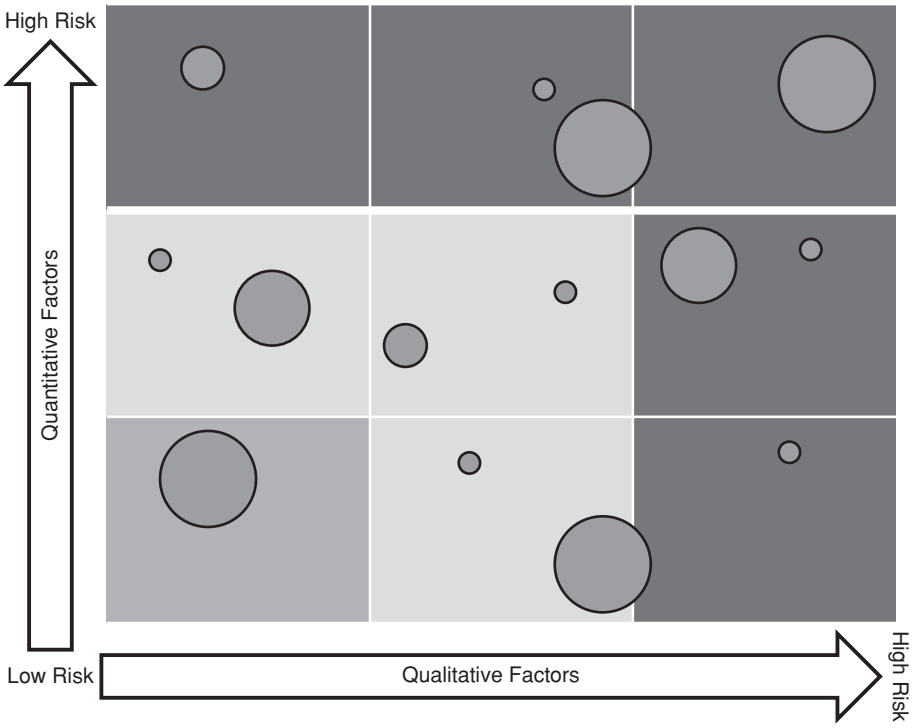


EXHIBIT 28.2 Portfolio Risk Assessment

partners. It is important to have a consistent understanding of a business partner's process and controls around contract-reporting requirements as well as a business partner's contract interpretation. Through effective communication, the common differences and disputes that arise from these areas can be mitigated. Also, consistent communication can even potentially expand the business relationship through identification of broader or new application of the contracted elements.

Incorporate Contract Terms that Improve Compliance

To improve contract compliance, it is important to ensure that contracts follow four simple rules:

1. Compensation terms should be equitable and clear.
2. Reporting requirements should include enough detail to increase transparency into the relationship.
3. Noncompliance should be penalized.
4. Include the right to audit.

To ensure that compensation terms are equitable and clear, contract partners need to take careful consideration of the future of the business relationship as well as the current state, so that to the extent possible, the contract terms can be defined

to create fairness in the short term as well as for the life of the contract. For example, in a licensing relationship, the licensee and licensor can negotiate compensation (royalty) terms that can be structured as a fully paid-up license, periodic payments, per-unit or per-use license, or a percentage-of-revenue or sale-related license. In most situations, each of these payment structures are intended to provide the licensor overall compensation for the use of the intellectual property. Although not always the right solution or even feasible, a percentage-of-revenue or sale-related license structure typically allows the two business partners to share directly in the success or failure of the use of the intellectual property. Thus, it is important for business partners to remember that no matter what the contract is that is being considered, as business environments change, the structure of compensation terms in a contract can have a significant impact on how much of the overall value of the contract is shared between the two business partners.

Also, successfully negotiated contracts have clearly reportable financial terms. The more detail that can be shared around the financial terms between the two business partners the more it can increase the transparency in the actual business and trust in the business relationship. In fact, detailed reporting can allow a business partner to perform simple data analytics and either become more comfortable with what is reported or assess and identify potential compliance issues. In fact, most contract disputes between business partners are as a result of differences in contract interpretation, mainly related to the financial terms of a contract. Examples of some of the most common financial-related contract terms that are disputed between business partners are as follows:

- Transfer pricing versus third-party pricing
- Most-favored-nations pricing or terms
- Allowable contract territories
- Allowable deductions or gross-to-net calculations
- Cost-plus margin pricing

To reduce the number of potential questions or disputes around these terms, business partners need to be as specific as possible when defining the financial terms in these self-reporting contracts. Furthermore, it is recommended to consider including hypothetical calculation examples into the actual language of the contract to provide additional clarity to the intention of the contract term.

Frequently, the only way to effectively reduce the frequency of noncompliance is to penalize contract partners for not reporting accurately and completely. Many companies that do not incorporate compliance-related penalties may incur financial or economic harm without a method to remedy these damages or even help encourage future compliance from business partners. In fact, in some extreme cases, business partners take advantage of that lack of compliance-related penalties, and the lack of payment from a business partner results in the equivalent of an interest-free loan or an incentive of noncompliance for business partners.

Finally, it is important to include a contract audit (also known as a contract examination, investigation, or assessment) clause in self-reporting contracts so that further transparency into the relationship can be obtained and overall compliance can be verified. In a majority of contractual relationships, compliance cannot be validated without an audit of the information that supports what is ultimately reported by the

business partner. An effective audit clause identifies the frequency that an audit can take place, an example of the specific information that is to be provided to the auditor, and the party that is responsible for the audit costs. In many contracts, the audit clause states that the initiating party is responsible for the audit costs unless a certain level of noncompliance is determined by the audit. It is important to consider all of these factors in an audit clause because it can encourage contract compliance.

Robust Outside Contract Examination Program

As discussed earlier, the outside contract examination (also frequently referred to as the *contract audit*) is an integral part of a successful contract compliance program. In most business relationships that are bound by a self-reporting contract, true transparency and trust in the relationship as well as assurance in compliance cannot be obtained without using outside contract examinations. A contract examination can take many forms: forensic investigation, limited scope, and agreed-upon procedures. The specific circumstances of the relationship as well as the companies involved will dictate the appropriate examination form. No matter what form the examination takes, an outside contract examination is certain to better assess contract compliance and help build transparency and trust and facilitate a more effective business relationship.

In addition to improving effective business relationships, outside contract compliance examinations can send a positive message to the market by helping other business partners understand that compliance is an important element of the business relationship. Contract examinations can also improve reporting controls and reduce revenue leakage and overall contract costs. The incremental revenue and reduction in costs can be the results of the recovery of actual, past contract partner noncompliance, as well as reducing future compliance risk. Overall, outside contract examinations can be a way to successfully recover incremental revenues and improve contract and overall shareholder value.

THE ROLE OF THE FORENSIC ACCOUNTANT

The forensic accountant can play an important role helping companies reduce contract compliance risk and increase the overall value of their contract portfolio. Much of the value that a forensic accountant can provide is in the area of outside compliance examinations. In addition to outside examinations, however, an effective forensic accounting team can provide assistance to companies implementing a robust internal and external contract compliance program.

The first step to an effective outside compliance examination is the selection of the appropriate business partner to examine. In some cases, those business partners that seem to pose significant risk to the business relationship are obvious; in others, a comprehensive contract portfolio risk assessment is the best way identify risky business partners. A company looking to perform a portfolio risk assessment can collaborate with a forensic accounting team that has extensive experience in contract compliance and that can add the knowledge of those quantitative and qualitative risk factors that should be used in this risk assessment (a brief overview of this risk

assessment is provided earlier in this chapter). In addition to providing the right risk factors, an experienced forensic team might even have direct experience with the contract business partners.

After a business partner is selected for examination, it is important for the forensic team to request the relevant data as well as identify the best persons to interview. The purpose is to gain the information needed to focus efforts in the areas of greatest compliance risk. In fact, a forensic approach to a contract compliance examination is one that focuses typically on what is not reported by the company being examined in addition to the information and documentation reported. As in most self-reporting contracts, only a limited amount of data are shared between contract partners. Even though some compliance issues can be identified through analysis of the information that is shared, most of the compliance issues are identified after a forensic accountant extracts the underlying data that support what is being reported to a business partner, as well as some of the indirect business factors that could affect what should be reported. To illustrate this point using a simple example, in a licensing contract in which the licensee is using the licensor's intellectual property to manufacture and sell a product, a licensee will normally provide sales information as support to the amount of royalties paid. Unfortunately, sales information does not always provide enough detail to understand all of the uses and value extracted from the licensor's intellectual property, such as product provided to customers or employees at no cost, products bundled with non-royalty-bearing products and up-front payments made by licensee's customers for a future opportunity to purchase royalty-bearing products. Since most of the risk and compliance issues usually are found within the information not reported, a forensic accounting team can maximize the effectiveness of the examination from a cost-benefit perspective by focusing on this information.

As the forensic team compiles data and information from the company being examined, one very important element to the examination is confirmation that the data provided by the company are complete. Many times the company examined extracts special reports for the forensic team and fails to provide documents that are used in the ordinary course of business. A forensic team is most interested in validation of the information used to support what is reported, and thus the best way to confirm this is to compare what is reported to business documents prepared and used in the normal course of operations. The forensic accountant can use various documents to accomplish this, including, but not limited to, accounting and financial reports, subsidiary ledgers of sales and accounts receivable, production records, inventory records, shipping records, general ledgers, and audited financial statements.

In many examinations, the company being examined is concerned that the ordinary course of business documents and information requested by the forensic team cannot be extracted effectively from its accounting systems. In these circumstances the use of forensic technology expertise can help. This expertise is a very effective way to overcome some of the typical objections that are raised by the company being examined.

After the forensic team obtains the necessary data to complete a successful examination, it is important to leverage all of the results from the examination to enhance the overall objectives of the compliance program. For example, the expertise of the forensic accountant and the results from effective compliance efforts can

provide more transparency in the business relationship with regard to each business partner's current understanding of the contract, the controls necessary to comply with the contract, information needed to best monitor future compliance, and a significant increase in the overall value extracted from business relationships.

GOVERNMENT CONTRACTING

The U.S. government is widely known to be the largest buyer of goods and services in the world. State and local governments also make up a large portion of purchased goods and services in the United States. Foreign governments also spend billions buying goods and services. Government spending has been a significant portion of gross domestic product for over a century, and the current trend in both the United States and worldwide is for increased government spending. Many countries have periodically adopted government stimulus programs, most recently in response to the credit market collapse of 2008, to help grow their economy and create jobs. In the United States, under the American Reinvestment and Recovery Act of 2009, the government appropriated $787 billion for this purpose.

Government contracts, grants, and cooperative agreements are frequently large dollar amounts, require performance over multiple years, include complex terms and conditions, and are highly regulated because they are funded with public money. Hence, disputes and litigation often arise in the course of government contracting that require knowledge of the applicable laws and regulations, understanding of an organization's processes and systems, and complex financial analysis. Government contract laws and regulations apply throughout the contract life cycle and at all functional levels of the performing organization, including operations, finance, accounting, human resources, and technology.

Because of the size and complexity of government contracts, grants, and cooperative agreements, and the abundance of applicable laws and regulations, forensic accountants are needed to support counsel in their defense of matters brought about by government agencies against contractors. Forensic accountants are also used to assist in actions brought against the government by contractors, and in disputes between parties that are government contractors. In government contracting, forensic accountants provide support to contractors and their counsel in three areas: risk and compliance, recovery, and crisis management and litigation.

RISK AND COMPLIANCE

Federal, state, and local governments include myriad laws and regulations in their contracts, grants, and cooperative agreements. The federal government imposes laws and regulations such as the False Claims Act, the Truth in Negotiation Act, Federal Acquisition Regulations, Cost Accounting Standards (CAS), the Davis-Bacon Act, the Competition in Contracting Act, and the Buy America Act. Many state and local government agencies impose federal laws and regulations as well as their own. The U.S. government also imposes complex requirements in many of its contracts such as the specialty metals clause, which prohibits the use of foreign specialty metals on goods intended for use by the Department of Defense.

Noncompliance with these laws and regulations poses a great risk to contractors and recipients of government funds. These can be financial risks such as monetary payback to government agencies; contract price adjustments and contract terminations; fines, penalties, and interest; and withheld payments. Noncompliance can also cause significant financial risk to government contractors and recipients of government funds such as being suspended, or debarred, from participating in future government activity. The financial risk here can be significant if the contractor or recipient depends on government activity for a significant amount of its business, and could affect its ability to continue as a going concern.

Doing business with government agencies also poses reputational risks to contractors and recipients of government money in the form of negative media coverage and potential criminal action taken against the contractor and its employees.

For example, noncompliance with the False Claims Act could arise when a contractor submits invoices to the U.S. government that include costs that have not been incurred, or have not been incurred for the contract to which they are charged. The contractor can be subjected to a fine of up to $11,000 per fraudulent invoice, a downward contract price adjustment or a terminated contract, and forfeiture of all open claims on the contract. The government will oftentimes also look to take criminal action against individuals involved in the fraudulent activity.

Forensic accountants can help contractors establish a government contract compliance infrastructure. They can also provide an assessment of the contractor's current practices and systems, and help remedy any deficiencies. This proactive approach is important for contractors to avoid negative publicity and the monetary impact of noncompliance.

Forensic accountants can also assist contractors with responding to specific government audit findings and allegations of noncompliance, and either help defend the contractor's practice as compliant, or help it remedy any deficiencies and quantify the impact to the government.

Government agencies have issued detailed guidelines for cost estimating, cost accumulation, and charging (billing) that must be followed. The U.S. government issues a set of federal acquisition regulations (FAR), which applies to all of its agencies, both civilian and military. The FAR is a comprehensive set of regulations that covers topics such as contract bidding and negotiation, pricing, commercial item contracting, allowable costs, domestic and foreign sourcing, and contract changes. The specialized knowledge of the forensic accountant is needed because of the detail and complexity of these regulations, and the fact that they are not always aligned with other recordkeeping requirements, like Generally Accepted Accounting Principles (GAAP) and the tax codes.

RECOVERY

Government contracts, grants, and cooperative agreements are unique in that changes to the original terms and requirements are routinely made, both before the contract is executed and consistently throughout contract performance. Changes can be directed by the government, or they can arise out of contract performance. The government includes a changes clause in most of its contracts, grants, and cooperative agreements.

Under its changes clause, the government provides contractors a means to recover any additional costs that are the result of changes to the initial order or alterations necessary to deal with unforeseen conditions. Changes can be quantity adjustments, revised scope or work requirements, alterations to deliverable goods and services, or administrative changes such as shipping and invoicing instructions. A contractor can propose or request an equitable adjustment to the contract, grant, or cooperative agreement for any additional costs, and negotiate a modification. If the changes to the contract create a greater risk to the contractor, they can propose a higher profit margin in their request for equitable adjustment. If a change results in lower costs, reduced risk, or a reduction in either contract price or funding requirements, the government is entitled to receive the reduction, and the contractor is obligated to disclose any reductions resulting from changes.

Contractors and the government do not always agree on what constitutes a change, and often disagree on the root cause of the change as to whether it was the contractor's performance or the government's actions. The government may believe that a certain requirement is not a change, but included in the existing requirements, and the contractor disagrees. Thus, a dispute arises.

The government includes a disputes clause in most of its contracts, grants, and cooperative agreements. Under its disputes clause, the government defines the process for resolving disputes, and the forum in which disputes are resolved. The contractor now has a claim instead of a proposed equitable adjustment.

Disputes typically occur when the contractor's performance is questioned or challenged by the government, and the contractor attributes performance issues to government activity or inactivity. For example, the government may attribute a schedule delay to the contractor's inability to order and receive critical parts from vendors necessary for contract performance. The contractor may counter that the schedule delay is due to the government making numerous changes to the requirements that resulted in changes to the purchased parts and corresponding vendor delivery delays.

Forensic accountants are useful to help contractors recover costs related to changes and disputes. Forensic accountants conduct financial analysis of costs incurred related to changes, assess the impact of contract changes to both the contractor and the government, analyze contract performance to determine the root cause of changes and increased costs, and quantify damages caused by performance.

The government has the right to terminate a contract for its convenience. A contractor is entitled under a termination for convenience to recover cost it has incurred for the terminated contract and has not been reimbursed for. Contractors may also be entitled to recover costs that continue after termination, such as unexpired leases, and costs related to assets that have lost useful value as a result of the termination.

Forensic accountants can help a contractor maximize its recovery of costs, investments, and profits in a termination for convenience by quantifying incurred costs, reclassifying costs, and interpreting contract requirements. If a contractor does not perform under the terms of its contract, the government can terminate the contract for default. Under a termination for default, the contractor is not entitled to recover unreimbursed contract cost, and may also be liable for reprocurement costs if the government needs to use another source for the goods or services acquired under the contract terminated for default.

Contractors will oftentimes contend that their performance on the contract was not in default of the requirements, and will work with their counsel to either reinstate the contract terminated for default, or convert it to a termination for convenience. Forensic accountants are used to support counsel with assessing contract performance, and help them build a sound defense against the government's position that the contractor was in default. Forensic accountants are also used to help mitigate contractor damages caused by the default termination.

CRISIS MANAGEMENT AND LITIGATION SUPPORT

As discussed earlier, doing business with a government agency involves contracts, grants, and cooperative agreements that are highly regulated and funded with public money. Compliance with the numerous regulations governing such projects is critical for success, and effective compliance with these regulations is essential to maximizing recovery of costs and earning profits, and maintaining eligibility for future government awards.

Government contractors and recipients of government funds are sometimes faced with government allegations of fraud, waste, and abuse, noncompliance with regulatory or contract requirements, and deficient or inappropriate activity while performing on government contracts or funding arrangements.

Forensic accountants are used to support contractors and their counsel in defending against government and whistleblower allegations, supporting their strategy when they are a plaintiff in an action brought against a vendor, subcontractor, or third party under a government contract, and helping prepare proposals and claims to the government.

Examples of the types of services forensic accountants provide to government contractors and funding recipients and their counsel include:

- Providing expert testimony on accounting compliance, contract performance assessments, and best practices
- Serving as a fact witness to support financial analysis, damage quantum, and proposal and claim preparation
- Providing financial analysis based on a specific contract interpretation communicated by counsel
- Refuting or challenging an opposing expert's testimony
- Conducting an investigation to detect the possible existence and extent of fraud, waste, and abuse
- Assessing the financial impact of any fraud allegation, and assisting with remedial actions to curtail exposure to a recurrence of problems or to prevent future improper activity
- Assisting in the preparation of proposals, claims, equitable contract price or funding adjustments, and termination settlements, including preparing supporting documentation and assisting with government audits
- Assisting with responses to government audit findings, including preparing position papers, and providing financial analysis to quantify and mitigate damages

- Assessing an organization's government contract compliance environment, and helping the organization to remedy deficiencies and establish a compliance infrastructure necessary to do business with government agencies

An example of how forensic accountants can help in the area of compliance is with the issue of how indirect costs are allocated to contracts. This is a common source of government audit findings and disputes between the government and contractors. Government auditors will make a determination that a contractor's allocation basis for certain types of indirect costs is not in accordance with CAS and FAR. They often cite that the allocation basis does not represent a causal-beneficial relationship between the cost and allocation recipient.

Forensic accountants can help support an allocation methodology by helping demonstrate the causal-beneficial relationship of the costs. They can also assist with determining an appropriate allocation basis for a specific cost or pool of costs. How home office or corporate expenses are allocated to business segments is prescribed in CAS 403, and frequently audited by the government. The government may determine that certain corporate expenses should be directly allocated to a specific business segment, and forensic accountants can help demonstrate that another allocation methodology is more homogeneous and better represents the relationship of the cost and the beneficiaries (the premise of CAS 403) than a direct allocation to one beneficiary.

Another example of how forensic accountants can help maximize the recovery of costs is helping a contractor prepare a settlement proposal for a contract terminated by the government for its convenience (as prescribed in FAR, Part 49). In one case, the government partially terminated a contract to build a ship, and the portion of the contract that continued was changed from building a ship to managing several subcontractors whose efforts were not terminated. Also, the contract had been stopped (delayed) before being partially terminated and changed.

Forensic accountants helped the shipbuilder prepare a delay claim to recover costs incurred during the 90-day delay period when contract work was stopped by the government. These costs included unabsorbed overhead, storage costs, severance pay, and idle capacity costs. When the contract resumed, it had been partially terminated in that the government changed the scope from building a ship to managing the efforts of several subcontractors whose work the government wanted continued. Forensic accountants helped the shipbuilder prepare a termination settlement proposal to recover unreimbursed costs for the terminated portion of the contract such as inventory, subcontractor efforts, and other costs such as loss of useful value of fixed assets. This involved reclassifying the nondepreciated (net book) value of various assets that were capitalized, but because of the termination of building a ship had become useless to the contractor; it thus became directly chargeable to the terminated contract. Forensic accountants also assisted the shipbuilder with repricing the continuing portion of the contract in an equitable adjustment proposal that included recapturing its investment and recovery of costs associated with accelerating other work in the shipyard to offset termination costs such as idle capacity and severance.

A third example of how forensic accountants can help in a crisis or litigation situation is in proving the correct charges for incurred costs. The government alleged that a contractor was submitting false claims by incorrectly charging costs incurred for another contract that was over budget (and unrecoverable) to a contract that was

under budget. Forensic accountants were used to validate the actual costs incurred for both contracts, including the correct allocation of indirect costs, and helped quantify the amount overcharged to the government. Forensic accountants also helped quantify the impact of the false claims on the contractor's audited financial statements, and helped with the disclosure of the prior period adjustment of reported earnings and profit.

In summary, all of the preceding services are conducted against the background that government agencies issue detailed cost accumulation and charge-out guidelines that must be followed, such as the FAR. It is because of the detail and complexity of these regulations, and the fact that their requirements are not always perfectly aligned with other recording and reporting requirements like GAAP, that the specialized knowledge of the forensic accountant is called for.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 29

Other Dimensions of Forensic Accounting

Michael S. Markman, Aron Levko, Mark W. Haller, Robert W. Dennis, Mona M. Clayton, J. Christopher Dineen, Dyan Decker, and Shane Sims

Some believe that all forensic accountants perform financial crime investigations. This view is explained largely by the fact that in the post-Enron, post-WorldCom era, forensic accounting has for many become associated solely with fraud detection and investigation. In reality, forensic accountants offer a much wider range of services. Although this book is focused predominantly on the deterrence, detection, investigation, and resolution of corporate fraud, it makes sense to offer here a chapter-length overview of some other dimensions of forensic accounting.

In their day-to-day practice, some forensic accountants focus on commercial disputes in specific industries or practice areas. In commercial disputes, forensic accountants typically play three roles: expert witness, consultant on technical accounting or financial issues, and arbiter of facts. As an arbiter or trier of facts, sometimes referred to as *special master*, forensic accountants are appointed by the court to act as judge and jury. In their consulting role, forensic accountants may provide discovery assistance, prove business facts, compute damages, and assist counsel in the development of strategy. One should not assume that a forensic accountant involved in commercial dispute projects is qualified to perform financial crime investigations. For an inventory of the skills to look for in selecting a forensic accountant who focuses on financial crime investigation, see Chapter 7. Close attention should be given to the individual's qualifications—including certifications and especially experience—before deciding on the right forensic accountant for the task at hand. Assuming that all forensic accountants are interchangeably capable of executing all forensic accounting investigation engagements would be analogous to assuming that all certified public accountants are qualified to prepare tax returns.

While fraud can be sensational and garner headlines, commercial disputes as well as, say, marital disputes among high-net-worth individuals occur often, may entail billions of dollars, and may involve complex issues requiring expert analysis. The majority of forensic accounting work actually occurs outside of investigations in a wide range of specific practice areas. A glimpse of these areas, suggesting why forensic accounting expertise may be helpful, follows.

ENVIRONMENTAL ISSUES

The shock felt across the United States when the Cuyahoga River in Cleveland, Ohio, caught fire in 1969 or when the entire community alongside Love Canal, near Niagara Falls, New York, was evacuated in 1977 because of hazardous chemicals buried there has been converted into reasonably tough federal and state environmental legislation. The Comprehensive Environmental Response, Compensation and Recovery Act (Superfund Act); the Resource Conservation and Recovery Act (Hazardous Waste Act); and to a lesser extent the Clean Air and Clean Water Acts sometimes generate complex disputes in which forensic accounting expertise may be helpful.

Specifically, the cradle-to-grave provisions of the Hazardous Waste Act and the shared responsibility of successive owners in the Superfund Act mean that environmental costs and damages can occur quite suddenly and under the leadership of a management team that was not in place at the time of the event. As a result, companies seeking to limit, reduce, or eliminate the costs of cleanup may engage forensic accountants to help reconstruct and present the operations of the company during the period in question.

Suppose that the successor owner of a property that is now a Superfund site is sued for the cleanup of a certain chemical remaining there. By conducting a forensic investigation that demonstrates that it never bought, sold, made, or took possession of the chemical in question, the defendant in the litigation may be able to eliminate or significantly reduce its liability.

In the environmental arena, forensic accountants may be useful in helping to reduce fines levied by the U.S. Environmental Protection Agency under the so-called economic benefit model. While the government looks at the economic benefits that have accrued to a company for being out of compliance, forensic accountants look at and present historical expenditures that were made to achieve compliance. Such expenditures may be used to offset portions of penalties ultimately payable.

INTELLECTUAL PROPERTY

Intellectual property—consisting of patents, trademarks, copyrights, and trade secrets—represents a significant portion of corporate value. For many industries, patents and copyrights also represent an important barrier to entry. Yet even as many companies move to protect their intellectual property, they increasingly engage in technology-sharing agreements as well.

While all of these trends contributed materially to the quality of life and productivity gains, they sometimes create fertile ground for disputes, including litigation. Because intellectual property has unique characteristics, determination of damages may require complex analysis. For example, in an intellectual property infringement case, there may be claims of lost sales and profits. But infringement tends to have an impact on prices, competition, and quantities in the marketplace. Therefore, forensic accountants may often go beyond lost sales and find the additional losses associated with the effects of price erosion, reduced economies of scale, and the presence of competition, among other factors that might not have otherwise existed. In some disputes, forensic accountants may calculate what a reasonable royalty would

have amounted to had such a royalty arrangement been in place. This calculation often considers the large number of terms and conditions that typically appear in complex royalty agreements—for example, exclusive versus nonexclusive—and their economic implications.

Many disputes arise out of licensing agreements. Licensors of intellectual property, disputing the ways in which licensees use their rights, may claim damages as well as lost profits. Forensic accountants may be consulted to help establish the damages sustained by the licensor, as well as the lost profits resulting from actions taken by the licensee.

In the area of patents, owners of intellectual property may seek protection not just for specific technologies but also for fundamental processes and algorithms. For example, in 1991 Kodak paid $873 million to Polaroid in a patent rights dispute involving instant cameras and films.[1] The figure that forensic accountants had to establish in this case was the amount of profit that Polaroid had lost. Meanwhile, forensic accountants for the defendant were given the task of rebutting the argument of lost profits.

INSURANCE AND BUSINESS INTERRUPTION

Many insurance policies now include a professional fees endorsement. Many believe that the existence of these endorsements represents recognition on the part of insurers that the preparation of a claim in the event of a catastrophe and the resulting interruption of business involve a complex matter that generates a risk for the policy holder. Companies often retain forensic accountants to help them prepare claims, establish damages and losses, and, in some circumstances, rebut the arguments of the insurance company's forensic accountants.

One of the primary challenges often facing the insured is to put accounting information into a format that reflects how insurance policies are written. Specifically, while corporate accounting calculates profit and loss within a production framework, losses from business interruption claims are structured quite differently. In the context of a business interruption claim, loss represents the difference between what happened to a company following a loss versus what would have happened had the loss not occurred. In other words, but for the loss, how would the company have performed? Calculating loss in this fashion is often a multifaceted challenge that, while using accounting, also requires an understanding of factors such as the industry and company personnel. Forensic accountants are often able to reconstruct and estimate how a business might have performed had the insured event not occurred. This is usually compared with post-event performance, recognizing the changes in revenues and expenses that occur as a result of the disaster. Changes in the revenue and expense components can be complex because the operations of the business—from what it sells to where and how products and services are produced—can be fundamentally changed by the disaster that befell the company.

---

[1] Intellectual Property Library, *Polaroid Corp. v. Eastman Kodak Co.*, U.S. District Court District of Massachusetts, 17 USPQ2 d 1711 (Bureau of National Affairs, Inc., 2003), www.patents.com/apl/kodak3.pdf.

Forensic accountants may establish and calculate the company's sustained loss and also provide expert-witness services to defend their findings. The challenge is compounded by the activities of similar expertise on the other side of the dispute. Given that reality, forensic accountants acting on behalf of the plaintiff may adopt the pragmatic goal of fighting for the best possible result rather than an overwhelming victory.

MARITAL DISSOLUTION

The incidence of divorce between spouses with substantial wealth often creates several challenges in setting entitlement awards as well as the valuation and division of marital property. For example, when there is a prenuptial agreement, such contracts often specify entitlements based on the living expenses of each spouse. Thus, in a marital dispute, the calculation of the entitlement may rely on estimating these expenses. A complication: The spending patterns established during the marriage often reflect joint expenditures. Forensic accountants may help analyze and separate historical spending to provide a basis for and defense of a proposed entitlement.

Apportionment of marital assets may present a number of challenges, compounded by whether or not the divorce is occurring in a community property state or an equitable distribution state. Questions may arise as to the value of assets that were initially brought into the marriage (premarital assets), their current value, and the portion of the marital estate they now represent. The task of apportionment of assets may lead to the work of tracing assets to determine who acquired them initially and how and of ensuring that all assets are taken into account during the apportionment process. The location of assets not disclosed by a spouse may materially weaken a proposed apportionment or give rise to dispute over a proposed settlement. Forensic accountants may be helpful in bringing important facts to light.

Forensic accountants may also address the value of professional goodwill in cases of marital dissolution in community property states. There is a wide range of valuation techniques for professional goodwill. Establishing a value for this asset—or determining whether it even exists—may have a material impact on the apportionment of marital assets.

SHAREHOLDER LITIGATION

Three federal securities acts create the framework in which interstate securities transactions are regulated. These are the Securities Act of 1933, the Securities Exchange Act of 1934, and the Private Securities Litigation Reform Act of 1995. Together, these laws attempt to ensure that the investing public has sufficient information to enter knowledgeably into securities transactions. Although each law defines a different standard of recovery for investors, the three share a common goal: to make the plaintiff whole through a reversal of inappropriate transactions or through monetary compensation of losses stemming from the violation or infraction of the law.

In general, the remedy of monetary compensation requires forensic analysis to best estimate damages. There are several widely accepted techniques for estimating damages. One of the most widely employed is the so-called out-of-pocket measure,

which is the difference between the price paid for a security and the actual value at the date of the sale. While this approach is easily understood, its application is often complex. Forensic accountants can estimate the value of the security in question, absent the alleged fraud or misrepresentation that provoked the action to begin with. The process often requires analyses that take into account macroeconomic information as well as industry and company-specific information. A more numerical, statistical approach to valuing securities uses linear regression analysis.

Shareholders sometimes file lawsuits against corporate officers and directors for violation of securities laws in addition to a wide range of other alleged offenses, including breach of fiduciary duty, personal appropriation of corporate opportunities, discrimination, self-dealing, oppression of minority shareholders, and violation of environmental laws. The majority of suits are brought against directors for the first alleged infraction in the preceding list: breach of fiduciary duty. In such suits, forensic accountants may be engaged to evaluate the causes of a business decline and assess the relationship of that decline to a board's decisions and performance.

BUSINESS VALUATION

The concepts and principles of business valuation for litigation purposes are the same as those for business valuations pursuing other purposes such as a buyout, creation of an employee stock option plan, or an equity investment. Business valuation in litigation may frequently occur as a result of marital dissolutions, dissident shareholder disputes, corporate dissolution, or a taxable transaction that is subsequently challenged by the Internal Revenue Service or other taxing authorities.

Forensic accountants engaged to clarify such situations often perform intensive data gathering in regard to the financial, contractual, legal, operational, and historical dimensions of the business under review. That information may be used to develop valuations under a number of generally accepted techniques, including market comparisons, discounted cash flow, net assets, comparable transactions, and comparable sales. Because disputes can arise with shareholders of different classes, the analysis often goes beyond the aggregate determination of value. In many instances, forensic accountants take into account the rights, privileges, and restrictions on various equity securities and assign values to each class.

Forensic accountants sometimes value preferred shares as well as pure equity securities. In such instances, the focus of analysis usually shifts toward a risk-based examination, in which forensic accountants evaluate a company's ability to make preferred-share payouts based on the presence of other fixed-payment obligations and other short- and long-term debt.

BUSINESS COMBINATIONS

Some business combinations provoke disputes related to antitrust laws, while others may generate disputes because of clauses in merger and acquisition contracts and the effects they have on purchase prices. In the former arena, plaintiffs establish harm from the anticompetitive effects of the defendant's antitrust violations. Forensic accountants may be engaged to help plaintiffs prove, and defendants rebut, alleged

damages stemming from restraint of trade. Restraint of trade can take numerous forms, including monopolization, exclusive dealing, price discrimination, and mergers that substantially lessen competition, among others. In many cases, success may rest on testimony and analyses by forensic accountants, who may be able to demonstrate lost profits based on a competitive impact analysis, market definition analyses by product and geography, and price elasticity in the marketplace.

Of course, not all business combinations provoke antitrust claims, but merger or acquisition contracts may generate disputes between buyers and the sellers—for example, disputes that arise from irregularities discovered after closing, the application of offsets, notices of objection immediately following closing, interpretations of materiality, and earn-outs. Those are just a few of the possible grounds for dispute. Forensic accountants may assist one or both parties in formulating the dispute, discovery, analysis, and calculation of damages. In litigation connected to merger and acquisition activity, there can be a high degree of subjectivity because of the personal involvement by the principals in the transaction. Forensic accountants may be helpful in such situations: They have no emotional involvement in the transaction. By providing objective, unbiased analysis, they may help move disputes toward resolution.

CYBERCRIME

In the current environment, a security breach may more likely refer to the attack and penetration of a computer network or a corrupt insider with authorized access to sensitive data than to a masked intruder on the premises after hours. The sources of these incidents range from sophisticated and well-funded state sponsors and organized crime groups to disenchanted or recently terminated employees. During an economic downturn, the likelihood of the latter could increase.

When an electronic breach occurs, cyber-security specialists and forensic technologists may be retained to determine the point of weakness in a business's information systems to determine what information was exposed or actually stolen, to find digital evidence that could aid in identifying the culprits, and to implement remedies that could prevent a comparable breach from occurring in the future.

Often, however, a cyber-attack has additional consequences. Forensic accountants may be called on to help quantify losses in support of civil or criminal litigation that may include costs to remedy information security weaknesses, replacement of plastic payment cards for customers and vendors, providing credit and identity theft protection, lost productivity, price erosion, impact to intellectual property, reduction in barriers to entry, and still other factors. During the course of litigation, forensic accountants and forensic technologists may serve as expert witnesses to establish facts and fact patterns associated with a cybercrime. Forensic accountants may also assist in the filing of an insurance claim associated with losses from cybercrime.

In the aftermath of a cybercrime involving service disruption or data theft, forensic accountants may be asked to help support the settlement of claims between a company and its vendors or customers. The existence of outsourced technology services often means that an attack and penetration result in liability for one or more companies providing technology services. Forensic accountants may be able to assist counsel in formulating claims specified by their technology outsourcing agreements.

The formulation of such claims is often complicated by the interdependent relationships among technology vendors. As a result, counsel may desire detailed analysis to support claims it is making on vendors. The reality and growing popularity of cloud computing is likely to increase the need for this type of forensic service.

Furthermore, cybercrime often involves the theft of data elements permitting an attacker to defraud identities or create a public perception that identities could be defrauded. Forensic technologists may be engaged to assess, evaluate, and quantify the potential or actual exposure of personal identities stored within the victim environment to assist legal counsel in preparing for, and defending against, a class action suit.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

CHAPTER 30

Corporate Remediation

Matthew J. Shelhorse, Christopher D. Barbee, Peter A. Viksnins, and Faizal B. Karim

WHAT IS REMEDIATION?

Remediation is the act of correcting a fault or curing a deficiency. Consider the traditional concept of a remedy—or rehabilitation—as an action taken to recover from sickness, to return to a state of health, and to pursue steps to prevent future illnesses. In the corporate world, such faults or deficiencies may lead to an inadequate control environment and increase the likelihood and magnitude of wrongdoing on the part of employees or third parties. In the modern business environment, remediation is often perceived as a dose of medicine—perhaps a distasteful one—but one that is required if a business intends to rehabilitate itself and return to a healthy state of corporate behavior.

Forensic accountants are, as described in this book, often called upon to assist various organizations in identifying, diagnosing, and addressing their issues—from delving into the company's books and records, to analyzing complex information technology systems, to interviewing management, and interacting with third parties. It is, therefore, not surprising that forensic accountants are more and more frequently asked to assist in corporate remediation efforts, considering their firsthand knowledge of the symptoms, underlying causes for the perceived weaknesses, and measures that can be taken to strengthen a company's internal controls, processes, and approach to managing risks in today's complex environment.

Corporate remediation efforts are undertaken—either voluntarily or as mandated by regulatory bodies in response to misconduct—to enhance or revamp a company's existing systems, internal controls, policies, procedures, and employee training that collectively create a corporate culture that values compliance in an effort to reduce the risk of misconduct in the future. Corporate remediation can cover a broad spectrum of business operations and regulatory issues from financial reporting and consolidation processes to tax reporting, import and export transactions, insider trading, terrorism financing, money laundering, and anticorruption compliance.

A comprehensive corporate remediation program incorporates controls intended to prevent and detect misconduct, as well as policies and procedures designed to respond to potential misconduct in an appropriate and timely manner. The goal is to establish and maintain a complete, effective, and sustainable antifraud and regulatory compliance program that enables the company to achieve its business

goals and maximize shareholder value in accordance with a compliance framework, consistent with company policy that adheres to relevant local laws and regulations.

Integral to these goals are cost considerations, wherein benefits from an effective compliance framework outweigh the costs associated with remediation efforts. Such benefits may be both quantitative and qualitative in nature and must be carefully identified, considered, and often communicated to the internal and external stakeholders of the entity. A strong case for corporate remediation should be made up front to successfully implement and execute a credible antifraud and regulatory compliance and remediation program.

WHAT IS DRIVING CORPORATE REMEDIATION?

Over the past decade, we have seen a perfect storm of events that have fueled the demand and need for forensic accounting expertise and services. These events include significant corporate compliance breakdowns and scandals, heightened media and public scrutiny of corporate and executive activities, changes in regulation and accounting standards, and proactive inquiries from regulators and governing bodies. Other forces at work during this time include business conducted in an increasingly global and electronic manner, complex business arrangements and transactions, and the cyclical nature of most economies.

In today's environment, organizations need to proactively identify and manage risks and areas of vulnerability. This process should include periodic assessments of key relationships, vendors, agents, alliance, and joint venture partners as well as monitoring compliance with key laws and regulations (for example, FCPA), hotline or whistle-blower complaints, and significant transactions. There is a need for experienced forensic resources to assist many organizations in addressing and mitigating the risks associated with today's challenges in a timely and effective manner.

Now, more than ever, corporations and their counsel realize the benefit and value of involving forensic accountants as key business advisors in a variety of situations, including the management of crises, assistance with M&A transactions, and the assessment and improvement of business performance and key processes.

Increased attention on corporate remediation is, simply put, a by-product of increased regulatory enforcement and public scrutiny of corporate behavior. We have witnessed several bellwether crises that have resulted in a public outcry for corporations to reform their behavior.

A series of economic crises arguably spawned regulatory efforts such as the USA PATRIOT Act of 2001, the Sarbanes-Oxley Act of 2002 (which created the Public Company Accounting Oversight Board, or PCAOB), the Fraud Enforcement and Recovery Act of 2009 (FERA), and a plethora of continuing economic sanctions and control programs in areas such as antitrust, government contracting, and export controls. The identification of fraudulent activity and the punishment of those entities and individuals in violation of the law has become a front-and-center issue for many regulatory and government agencies, one that shows no signs of diminishing any time soon.

Beyond the borders of the United States, various countries and regional authorities have enacted legislation or regulations that affect worldwide corporate behavior. For example, the United Nations Convention Against Corruption (UNCAC)

entered into force on December 14, 2005.[1] According to the UN, 140 countries have signed the treaty.[2] Furthermore, regulatory authorities outside the United States are themselves increasing enforcement efforts in areas such as antitrust, antifraud, and anticorruption. International regulatory bodies have also shown an interest in cooperation and sharing of information on global cases in a manner not previously seen.

For the antitrust area alone, as of July 2009, three-quarters of the way through the federal government's fiscal year 2009, U.S. criminal antitrust fines exceeded $950 million—more than the total amount collected in any fiscal year in the past decade (total fines for fiscal year 2008 were $701 million),[3] and also included the longest jail sentence ever imposed for a criminal antitrust case in the United States (48 months in the freight-shipping industry).

The following summarizes certain high-profile cases affecting the depth and breadth of today's corporate remediation efforts:

- *Enron (Financial Reporting):*[4] According to an SEC complaint, the ultimate demise of Enron was primarily the result of inadequate controls, disclosure, and transparency in its books and records.
- *WorldCom (Financial Reporting):* According to an SEC complaint, WorldCom overstated net income by $9 billion[5] by inappropriately capitalizing expenses or releasing reserves against operating expenses, among other inappropriate activities. The corporate failures at Enron and WorldCom led to widespread calls for changes in accounting standards and strengthening of corporate governance and oversight, and are widely considered to be the proximate cause of the enactment of the Sarbanes-Oxley Act of 2002, which includes stringent requirements for corporate governance as well as increased oversight over auditors by the PCAOB.
- *ITT Corporation (Export Controls):*[6] ITT, the leading manufacturer of military night-vision equipment for the U.S. armed forces, pled guilty to export violations, and paid over $100 million in fines and penalties, as well as implementing a remedial action plan and accepting an independent monitor.
- *Iraq Oil for Food (Anticorruption):*[7] In 1995, the U.N. adopted Security Council Resolution 986, which permitted the government of Iraq to sell oil and to use proceeds from those sales to purchase humanitarian supplies such as food for the Iraqi people. According to the report issued by the Independent Inquiry Committee into the United Nations Oil for Food program, in an extensive scheme, the Iraqi government solicited illicit payments in the form of surcharges from oil purchasers and kickbacks, often termed "after-sales service fees," from humanitarian goods suppliers. These kickback payments were masked by inflating

---

[1] www.transparency.org/global_priorities/international_conventions/projects_conventions/uncac.
[2] www.unodc.org/unodc/en/treaties/CAC/signatories.html.
[3] www.gibsondunn.com/Publications/Pages/2009 Mid-YearCriminalAntitrustUpdate.aspx.
[4] www.sec.gov/spotlight/enron.htm.
[5] www.sec.gov/litigation.
[6] www.treas.gov/press/releases/tg259.htm.
[7] http://iic-offp.org/story27oct05.htm.

the contract price by approximately 10 to 15 percent of the contract value. A substantial number of companies involved in this scheme were prosecuted and fined by the DOJ and SEC, including some of the largest and most prominent corporations in the world.

Changes in enforcement methods are also spurring increased remediation efforts, including the following:

- Exponentially increased monetary fines, penalties, and sanctions.
- Increased focus on individual criminal liability[8] in spheres of activity historically perceived as corporate crimes.
- Use of nonprosecution and deferred prosecution agreements that call for the imposition of independent compliance monitors that will oversee or analyze certain portions of a company's operations for a period of time.
- Expansion of enforcement efforts to entire industries or industry sectors. There have been industry-wide sweeps involving the oil and gas, medical device, and pharmaceutical industries, among others.
- Increased interagency cooperation within the United States as well as among global regulators[9] and the use of FBI agents and sting operations.
- Increased scrutiny of the acts of others (for example, agents, consultants, customs clearance providers).
- Increasing instances of voluntary disclosure, with the promise from regulators of tangible benefits that can be realized by companies that voluntarily disclose and subsequently cooperate with the regulators.

The basic principles of corporate compliance and remediation programs, however, are not new. These principles, as discussed elsewhere in this chapter, can be found in the U.S. federal sentencing guidelines,[10] the Internal Control—Integrated Framework, published in September 1992 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, and in a wide array of other compliance-related literature.

These fundamental tenets of compliance are the benchmark against which existing programs are compared to determine the compliance gaps that require additional analysis and remediation. Organizations looking to move to the cutting edge in this

[8] "Companies can absorb the cost of big fines and the hit to their reputations. . . the Justice Department is hoping for a bigger deterrent effect by targeting people rather than just punishing their employers. . . ." Mark Mendelsohn, deputy chief, Fraud Section, Criminal Division, Department of Justice, in Dionne Searcey, "Currents: To Combat Overseas Bribery, Authorities Make It Personal," *Wall Street Journal,* October 8, 2009.

[9] ". . . [T]he Department will continue to pursue vigorously violations of the Foreign Corrupt Practices Act. The Department does not simply react to self-disclosures and rely on internal corporate investigations. To the contrary, in this area, as in many others, the Department is being proactive and aggressive. . . . I fully expect that the number of FCPA prosecutions—of corporations and individuals alike—will continue to rise, as will the extent of our cooperation with foreign law enforcement partners. . . ." Lanny A. Breuer, assistant attorney general, Criminal Division, November 12, 2009.

[10] www.ussc.gov/2009guid/tabcon09.htm (See Chapter 8, Part B).

area can study these guidelines as well as corporate examples from recent years to assess how robust their own programs and systems are and in turn how vulnerable they may be to irregularities.

WHY IS REMEDIATION NECESSARY?

At the most basic level, corporate remediation efforts are expected by stakeholders and regulators alike. Shareholders expect transparency and good corporate citizenship, as amply demonstrated by numerous shareholder class-action lawsuits that allege that corporate management was aware of wrongdoing, but failed to disclose and remediate such wrongdoing. Under Sarbanes-Oxley, management is required to provide certifications relative to the quality of corporate internal controls. Auditors are required to opine as to the effectiveness of internal controls. Clearly, if remedial actions are lacking, management's certification, and the auditor's opinion, may be adversely affected. In many corporations, members of senior management have responded by having their direct reports provide similar certifications to them in connection with quarterly and annual financial reporting processes.

Corporate remediation—whether undertaken voluntarily or in response to misconduct—encompasses efforts to modify or streamline processes (or both) and procedures deemed necessary to reduce the risk of fraud occurring (or reoccurring) in the future. Remediation may result in changes to an organization's people, systems, control environment, and corporate culture, or a combination thereof. While personnel-related remedial actions may vary according to the severity of the circumstances, they are typically one-off decisions made in response to a particular incident, usually following an investigation of initial allegations of wrongdoing. Remedial efforts targeted at an organization's systems, control environment, and culture tend to be more proactive and forward looking in nature and hence are usually driven by a company's commitment to compliance on a long-term basis.

There is a continuing belief among regulators that adequate internal controls that are independently assessed on a periodic basis may help to control and mitigate corporate misbehavior. This was evident in the recent settlement between Bank of America Corporation (BoA) and the SEC relating to BoA's acquisition of Merrill Lynch. In that settlement, the SEC required that BoA retain an independent auditor to assess the controls and procedures relating to BoA's disclosure processes based on the criteria in COSO, in the same manner as internal controls over financial reporting must be assessed pursuant to Sarbanes-Oxley.[11]

One of the key starting points for many entities is to assess the nature, adequacy, and effectiveness of their overall compliance environment and program. Companies and boards of directors should start by asking some tough questions:

- Do we have the right tone at the top? Is senior management active and engaged in the compliance process?

[11] www.sec.gov/litigation/litreleases/2010/boaexanotice.pdf.

- Do we have a compliance officer? Is this a full-time position or does the individual have other responsibilities within the organization? Can this individual focus on the responsibilities and respond to matters in an adequate and timely manner?
- Do we have a dedicated compliance department or is this task adequately handled by others (for example, legal, internal audit, and human resources)?
- How are compliance issues raised within the organization (for example, hotlines, complaints, internal audit, and operations)?
- How many compliance matters does our team handle in a given month, quarter, or year? How have these matters been addressed and resolved by management? Have there been any recurrences of identified fact patterns?
- Are we incentivizing appropriate and desired behaviors in our personnel?
- Are appropriate disciplinary actions taken with respect to wrongdoers?

An effective compliance program should not only ensure compliance with laws and regulations and accuracy of financial books and records, but can also—to the extent that the public is aware of a corporate misdeed—restore a company's tarnished reputation with the public and its stakeholders and potentially reduce fines and penalties that may be levied by regulators. Also, companies with both ethical guidelines and effective compliance programs typically report suffering fewer economic crimes.

In addressing compliance violations, management must consider the root cause of the violation and whether there was a control failure or an intentional circumvention of established processes. Management is required to notify the audit committee and their independent auditor regarding why their controls failed and what sustainable procedures they have implemented to prevent recurrence. By implementing sustainable remediation procedures, progressive companies can protect corporate reputation and brand value, meet increased demands from a wide array of stakeholders, manage internal and external performance expectations, and strengthen the organization's ability to respond to increased legal and regulatory pressures. Companies operating within an effective control framework may experience the following:

- Enhanced availability and flow of information
- Stronger reputation as a company with sound governance procedures
- Fewer incidents of misconduct and noncompliance
- Greater assurance of ethical decision making
- Better detection and deterrence of unethical behavior
- Lower litigation costs

Benefits of corporate remediation are numerous and range from intangible benefits like reputational maintenance or improvement to quantifiable benefits such as cost savings obtained through avoiding imposition of a compliance monitor. Regardless of the situation, outlining the expected outcomes of a remedial action plan can aid a company more effectively and efficiently plan and monitor a remedial action plan. Intangible benefits and other benefits that cannot be easily quantified are simply too numerous to list and, though arguably as important as tangible or quantifiable benefits, may carry less weight in decisions primarily linked to a company's bottom line financial performance.

According to the Association of Certified Fraud Examiners *2010 Report to the Nation on Occupational Fraud and Abuse,* an estimated 5 percent of corporate revenue is lost to fraud. Implementation of robust internal controls should be a key component of any corporate remediation plan and can be a component that can reasonably be expected to more than pay for itself, particularly if future crises or even minor to moderate future losses are prevented.

Imposition of compliance monitors by regulators can be intrusive, costly, and often span multiyear periods. Compliance monitors typically report to regulators, do not work under attorney–client privilege, and must be paid by the company they are monitoring. Demonstrating to regulators before settlement that a company understands the importance of remediation and is committed to avoiding future violations through the implementation of a robust remediation program can be an effective means of avoiding the imposition of a compliance monitor. Also, the potential imposition of a compliance monitor can be a strong component of the case for a proactive corporate remediation plan.

Companies would be remiss not to consider the expectations of enforcement authorities when contemplating remediation, regardless of whether the remediation is reactive or proactive. Whether the area in need of remediation is export controls, anticorruption compliance, financial reporting controls, or another area, it is clear that regulators expect companies to implement remedial action plans that go beyond the paper upon which they are written and come alive in the organization to embrace the remedial actions intended to prevent and detect future illicit activity.

Many goals of remediation efforts are situation specific. Most, however, if not all, remediation plans seek to accomplish certain shared objectives. Among those shared objectives is the promotion of a corporate culture that values compliance (typically called *tone at the top*). In some cases, promotion may mean building from the ground up while in other cases it may mean pushing a corporate-level culture out to subsidiaries or integrating acquired or merged business units into the overall entity. Another such shared objective is the implementation of consistent internal controls and business processes across the entire organization—into various lines of business and across geographic territories, the benefits of which outweigh the costs.

HOW TO REMEDIATE

The seven elements set forth in the federal sentencing guidelines[12] provide the basic framework that forensic accountants can use to assist in evaluating and establishing a strong compliance program. These elements are summarized as follows:

1. *Develop Standards and Procedures*—A company must have standards and procedures, such as a code of conduct or a code of business ethics, that document the expected behaviors to be followed by company personnel as well as processes to be employed to prevent and detect possible misconduct.
2. *Knowledge and Operation of the Compliance and Ethics Function*—The organization's governing authority should be ultimately responsible for a company's

[12] www.ussc.gov/2004guid/8b2_1.htm.

overall compliance program and should ensure that the individuals leading the compliance program have "adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority."

3. *Exercise Diligence in Delegation of Authority*—A company's compliance program should use care not to include individuals who have previously engaged in illegal activity or misconduct. The organization should conduct some form of due diligence on potential candidates to identify such potential activity.
4. *Effective Communication and Training*—A company should communicate its "standards and procedures, and other aspects of the compliance and ethics program" to personnel on a periodic basis. In this regard, entities may conduct training programs for employees to provide real-life examples of the ethical dilemmas that may be encountered in the course of their work.
5. *Proactively Monitor and Test Activity*—A company must monitor the workplace and test its compliance functions in an effort to detect possible misconduct. In addition, a company must "have and publicize a system" for employees to report possible violations and seek guidance regarding ethical concerns.
6. *Implement Disciplinary and Incentive Mechanisms*—A company's compliance program should be "promoted and enforced consistently throughout the organization." The program should ensure that appropriate disciplinary actions are taken against employees "for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct." A company should also ensure that those who report violations are not retaliated against and that incentives are provided to personnel to conduct themselves in a positive manner that is consistent with the compliance and ethics program.
7. *Respond to Violations Appropriately*—A company must take reasonable steps after a violation has been detected "to respond appropriately to the criminal conduct and to prevent further similar conduct." This includes "making any necessary modifications to the organization's compliance and ethics program."

The role of senior management in creating and communicating both an ethical code of conduct and responsible behavior are crucial. Ownership of compliance rests with senior management, which sets clear expectations in regard to the company's worldwide compliance standards. Management's responsibility includes actively and continuously driving implementation within the entities, and ensuring that the right resources are available for implementation. One approach that has worked well for many companies is to establish a central team that can be available to assist local management by providing guidance and support when needed, supporting documentation, best practices in key compliance-sensitive areas, and insights with respect to frequently asked questions. Essentially, senior management is responsible for rigorous execution of the compliance framework and is required to centrally monitor and report the execution efforts to the board of directors and in certain cases, to external parties.

To continue with the medical analogy from the beginning of this chapter, the overall remediation process should involve a journey from illness to health. In remediation or consulting parlance, this is often referred to as the corporate shift from the current state (illness) to the future state or desired state (health). While simplistic, this objective should be kept in mind to avoid a situation in which the operation was

successful (development and implementation of a compliance program), but there was a recurrence or follow-up issues (compliance program not followed in practice). We understand, both from literature and project experience, that many corporations often face remediation or compliance fatigue from well-meaning, but potentially ineffective, compliance remediation methods that are forced on them from headquarters. If the compliance diet is too severe, draconian, or expensive, the odds of the patient sticking to it are lower. The compliance remediation program must be perceived as supporting healthy business objectives, rather than as an obstacle to those objectives.

As noted in the risk assessment flowchart that follows, the very first activity to be undertaken is the gathering of data. Often, forensic accountants will have already begun this activity in connection with their investigative role—but just as often, a separate team is engaged to perform remedial actions, for example, if remedial efforts are not being performed under the attorney work product doctrine or attorney–client privilege. In either case, the initial portion of the diagnosis must be undertaken with relevant and accurate facts. These data are typically gathered using traditional forensic accounting methods—targeted information requests from key departments and personnel, interviews of relevant knowledgeable personnel (these may run the gamut of corporate functions, from accounting and finance staff to human resources, legal, and operational personnel), and discovery and analysis of electronic and transactional data, which facilitates sample analyses for any patterns and trends that may be present.

The forensic accountant then examines the available data in light of the body of knowledge available that describes desired behavior—for example, if the initial data indicate that a fraud has occurred, the forensic accountant may consider the COSO antifraud internal controls, the Sarbanes-Oxley regulations, and the U.S. federal sentencing guidelines, particularly Chapter 8 of those guidelines, which describes the U.S. government's expectation of a robust compliance program. These materials include suggested antifraud control components such as diligence in the delegation of authority and periodic monitoring of the effectiveness of antifraud controls. The forensic accountant considers whether these components of the corporate compliance program were operating and effective during the period when the alleged fraud occurred.

In a broader sense, the consideration of corporate objectives and the potential impact of noncompliant behavior informs the forensic accountant about the existence and extent of risk factors as well as the possible materiality of issues that may arise. While a comprehensive overview of risk management is beyond the purview of this chapter, many of the concepts of that area of study are necessarily incorporated into corporate remediation. It is strongly recommended that any corporate remediation be performed under the auspices of a corporation's existing enterprise risk management (ERM) system, as such a system is designed to identify and mitigate those risks that are perceived as being the greatest threat to the achievement of corporate objectives. Furthermore, if a corporation has a strong ERM process in place, it is less necessary to create a new methodology simply for the purposes of remediation. (See Exhibit 30.1.)

Implementing effective control systems requires a comprehensive understanding of the sources of fraud or regulatory risk within the context of a company's domestic and global operations. The purpose of conducting a risk and control assessment

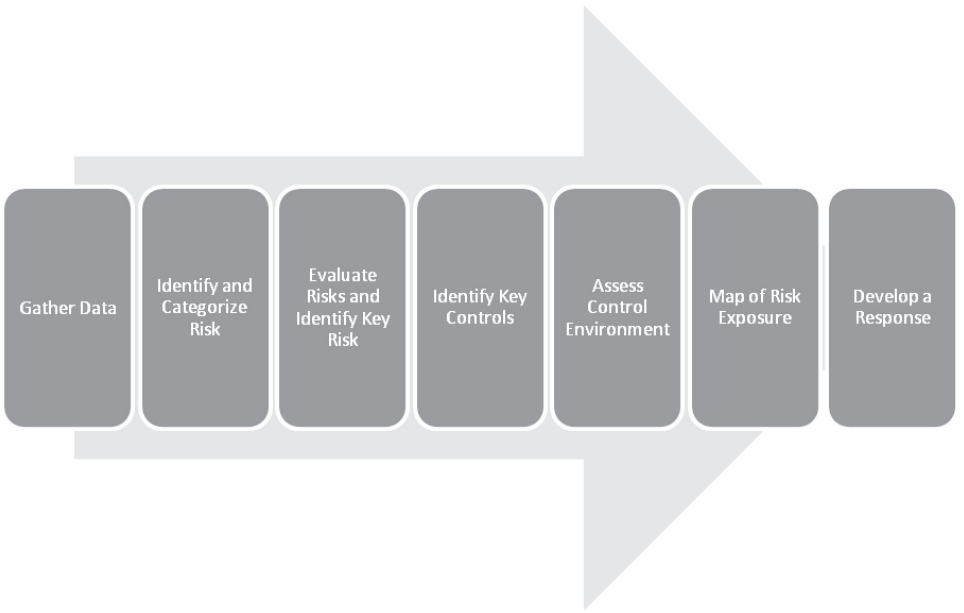


EXHIBIT 30.1 Risk Assessment Process

is to identify key risks that could threaten the process being assessed and evaluate whether the controls in place to manage key risks are effective. The assessment aims, in particular, to:

- Identify the risks that could threaten key processes and systems.
- Assess their likelihood and potential significance in regard to their qualitative and quantitative impact on the organization.
- Identify the key risks and assess the controls currently in place to manage such risks.
- Identify the remaining residual risks (after mitigating controls are considered).
- Summarize and map where the risks lie within the organization.
- Determine whether any control enhancements or improvements are required as well as any other remedial actions that could be taken to strengthen the control environment and structure.

Underlying the risk assessment process is an understanding among company personnel of the overall risks to which a given process is subject and their role in identifying and managing those risks on an ongoing basis and in a proactive manner.

This risk assessment process can take many forms, depending on the organization, the nature of its operations, its systems, and the availability of information. The key is to follow a methodology and process that can be documented, replicated, and explained to others. The following summarizes some of the items to be considered in connection with the risk assessment:

- Industry and third-party risks (that is, government customers, regulators, partners, vendors, and suppliers)
- Risks inherent in the business model (size, centralized or decentralized operations, anticipated growth)
- Joint ventures and alliances
- Transaction types
- Geographic location of business and third-party services to be performed
- Training of key personnel (for example, compliance, finance, legal)
- Prior audit findings, hotline reports, and related available information

ROLE OF THE FORENSIC ACCOUNTANT

As demonstrated in recent cases, successful efforts of remediation and the establishment of an effective and sustainable compliance program can be key factors in reducing possible fines and penalties. Learning from a crisis experience with the support of a forensic accountant can be critical to the success of a company's remediation plan.

A forensic accountant is trained and experienced in investigating and resolving suspicions or allegations of fraud through document analysis, including both financial and nonfinancial information, interviewing, and third-party inquiries, including research conducted through commercial databases. In the remediation process, a forensic accountant will play a key role by designing, testing, and assisting with the implementation of a compliance program. Forensic accountants also enhance the remediation process by identifying and investigating potential compliance violations. Examples of the types of services forensic accountants provide during the remediation process include:

- Performing a gap analysis
- Conducting a risk assessment
- Providing training and education
- Performing continuous monitoring activities
- Conducting detailed transaction testing
- Responding to regulatory inquiries and conducting investigations

In remediation efforts, forensic accountants will diagnose the issue by conducting a gap analysis. By assessing the condition of a company's current systems and compliance infrastructure, a forensic accountant can identify compliance gaps and make recommendations to increase or improve levels of compliance. A gap analysis is conducted by comparing documented procedures and actual practices to regulatory expectations or best practices or both. Forensic accountants will also observe the corporate code of conduct and existing policies that set the company's tone.

Forensic accountants assess compliance objectives and risks, while analyzing and benchmarking the company's current performance and control environment. Forensic accountants can gain unique perspectives when interviewing key executives and managers (that is, sales, legal, compliance, finance, internal audit, human resources, and information technology) and are better able to evaluate control designs

and assess operating effectiveness based on the information gathered during such discussions.

In addition to understanding a company through interviews, documented policies, and actual practices, a forensic accountant can assess the tools used in the current framework. A risk assessment can help a forensic accountant better examine the company's compliance program and evaluate risk areas. Risk areas can be addressed and recommendations implemented, but the company must seek to continuously train employees and implement and integrate new policies and procedures from the top down.

Training and education programs are an essential element in implementing successful remediation plans and in maintaining regulatory compliance on an ongoing basis. Forensic accountants can help determine training objectives based on their understanding of the company's compliance strategy and the identified enhancements. Based on a forensic accountant's regulatory and legal experience, they are able to develop targeted training materials that include rules and regulations, regulatory trends, red flags, compliance-sensitive items, and a testing approach that the company can employ on a periodic basis.

Upon implementation of the client's new policies, procedures, and internal controls, a forensic accountant will assess the local entity's progress with regard to implementation process and provide recommendations on the entity's policies, procedures, and internal controls. Monitoring is not a process solely used during and after a time of crisis, but it should be a continuous ongoing process for a company. Forensic accountants—experienced in investigating fraud and allegations of noncompliance—are often called upon as monitoring and remediation advisors to bring the forensic mind-set in assessing the client's programs at both a local and corporate level. The forensic mind-set refers to the combination of intellectual curiosity and professional skepticism that result from experience with, and training in, investigations of various types of potential fraud and misconduct. Consider the following recent example from a well-known global company.

For several years, the company sent its internal audit team, which lacked adequate forensic accounting experience or resources, to examine its operations in a specific emerging market. The internal auditors returned to corporate with a report of no findings of noncompliance with the company's ethics and anticorruption policies. One year, the compliance officer at the company's headquarters decided to conduct certain tests to monitor the overall compliance health of the company and retained forensic accountants to assist with the exercise. This analysis identified numerous indicators of potential noncompliance. In the resulting investigation to determine if the initial red flags represented real issues to the company, numerous violations of company policy were discovered and dated back over a period of years.

The preceding example is not intended to imply that internal auditors or compliance professionals should not be used to investigate allegations of fraud and noncompliance. On the contrary, these professionals are often called upon to investigate allegations of fraud and noncompliance, and can often do so in an effective manner as long as they have adequate forensic accounting experience and resources. If not, then the investigation team should include forensic accountants in order to have a well-balanced set of skills. Also, forensic accountants often team with the client's compliance personnel and internal audit team to develop test plans to assess certain locations, key controls, and relationships with local entity personnel. Technology

specialists also play a role in the monitoring process, by assessing the client's internal compliance and accounting systems such as dashboards and hotlines.

As part of the monitoring process, a forensic accountant often conducts site visits to local entity locations based on the results of the risk assessment performed. While onsite, a forensic accountant can test transactions in key compliance-sensitive areas and assess the local entity's compliance with company policies and procedures. Some key compliance-sensitive areas include:

- Political donations and contributions
- Use of agents, distributors, consultants, and other third parties
- Sponsorships
- Gifts and hospitality
- Travel and entertainment
- Transactions with government officials
- Petty cash
- Import and export

Detailed transaction testing not only includes reviewing the support for journal entries and ensuring transactions are appropriate in nature, but it may also include reviewing the local entity's contracts for the inclusion of certain clauses and provisions, compliance with company codes and policies, and the right to terminate the contract and to enforce audit right provisions. Furthermore, transaction testing may involve analyzing the processes surrounding the local entity's bank accounts. For example, a forensic accountant may analyze bank account documentation to determine whether the appropriate approvals were obtained before the withdrawal of funds. Detailed transaction testing is an essential step in the remediation process, as it demonstrates to management the areas in which additional training may be needed at the local entity as well as areas in which they have improved their processes and procedures.

The best well-known service a forensic accountant provides is responding to regulatory inquiries and conducting investigations. During the remediation process, forensic accountants assist or co-source (or both) with clients in responding to an issue or matter that may arise.

RECENT CASES

There have been many recent cases involving compliance investigations and related settlements. One of the recent landmark, precedent-setting matters involved Siemens AG and its efforts to address various corruption charges. Siemens resolved its FCPA charges with the U.S. Department of Justice (DOJ), the Munich Public Prosecutor's Office, and the U.S. Securities and Exchange Commission (SEC) with multiple guilty pleas and the payment of $1.6 billion in fines, penalties, and disgorgement of profits, including $800 million to U.S. authorities. This was the largest U.S. monetary sanction ever imposed in an FCPA-related case. Siemens was not, however, able to avoid the imposition of an independent monitor for a four-year period.

The DOJ and the SEC specifically noted and considered Siemens's substantial assistance, cooperation, and remediation efforts, which resulted in the DOJ's

recommendation that lower criminal fines be imposed. These fines could have been between $1.3 billion and $3.2 billion. In its sentencing memorandum, the DOJ stated:

> *The reorganization and remediation efforts of Siemens have been extraordinary and have set a high standard for multi-national companies to follow. These measures, in conjunction with Siemens' agreement to retain a Monitor (with support from a U.S. law firm with FCPA and compliance expertise) for a term of four years, highlight the serious commitment of Siemens to ensure that it operates in a transparent, honest, and responsible manner going forward.*

The settlement involved at least 4,200 allegedly corrupt payments totaling approximately $1.4 billion over a six-year period to foreign government officials in various countries, as well falsifying its books and records to cover up the payments. According to the DOJ's sentencing memorandum, the factors that enabled the corrupt payments to occur included:

- Insufficient antibribery compliance policies and procedures
- Inappropriate investigation and response to allegations of corrupt payments
- Failure to discipline employees involved in making corrupt payments
- Failure to establish a sufficiently empowered and competent corporate compliance office
- Failure to report looming and systematic problems to the audit committee
- Highly decentralized organization structure

Before its remediation efforts, Siemens reported a material weakness in its internal controls and failures in anticorruption-related policies and procedures. Specifically, the existing compliance policies and procedures did not address specific corruption risks and included only general principles and recommendations, not mandatory requirements. The compliance program was previously a paper program, meaning that while some anticorruption policies were adopted, Siemens employees were not sufficiently educated and trained with regard to these policies, new compliance policies were viewed as changes in form and not substance, and there was little effective monitoring or auditing of compliance policies. Furthermore, there was no evidence of the right tone at the top at Siemens, as there was not a clear message communicated throughout the organization by senior management that "Siemens would rather lose a business opportunity than win it through corruption."

In developing its remediation plan, Siemens identified the following areas of concern that would have to be addressed during the remediation program:

- Improper payments made or benefits provided (or both) to foreign public officials to obtain or keep business
- Use of third-party intermediaries as conduits for such payments
- Failure to perform proper due diligence on business partners
- Use of off-balance-sheet bank accounts or on-balance-sheet slush funds (or both) to make such payments

- Falsification of books and records
- Material weaknesses in internal controls over financial reporting

The objectives of Siemens's remediation program were to:

- Identify gaps in internal controls, policies, and related frameworks.
- Develop a standard set of antibribery internal control requirements.
- Design and implement antibribery internal controls at all business reporting entities worldwide and independently test those controls at all high-risk or material reporting entities (or both).
- Capture evidence to support the settlement process with the SEC and DOJ to demonstrate that sufficient progress has been accomplished to address the issues and reduce the risk of reoccurrence.

Through its remediation program, Siemens streamlined its organizational structure; overhauled and strengthened its compliance, legal, and audit functions; and addressed control gaps by changing its senior management, enhancing the tone at the top, targeting steps to address specific corruption risks, improving and dramatically expanding compliance programs, strengthening and consolidating the audit function, and enhancing internal controls. The DOJ commented that Siemens made "substantial compliance and remediation efforts."

REMEDIATION GOING FORWARD

As previously mentioned, the past decade witnessed several corporate crises that required companies to remediate in response to misconduct and pay penalties, fines, and disgorgement of profits due to regulatory enforcement. As a result of the record fines paid by Siemens (which may have been even greater but for Siemens's commitment and rigorous implementation, which was praised by regulators), remediation efforts going forward into the current decade may take a page from the Siemens chapter. While other companies may not require the same level of effort and intensity as has been shown by Siemens in its remediation efforts, it is clear that regulators give credit for a clear demonstration of commitment to compliance and a timely and strong response when misconduct is identified.

The DOJ and the SEC, recognizing that no compliance program is bulletproof, have made comments suggesting that they may forego prosecution of companies that maintain effective compliance programs despite the occurrence of a violation. Paul Berger, former associate director of the SEC's Division of Enforcement, stated publicly that the SEC, as a matter of policy, will not bring enforcement actions against companies that are able to show robust compliance procedures in existence at the time of the violation. In fact, the federal sentencing guidelines state that "the failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct."[13]

[13] www.ussc.gov/2009guid/tabcon09.htm (see Chapter 8, Part B)—Sentencing guideline.

When a resolution is reached with the DOJ after a violation is discovered, the existence of a suitable compliance program will allow for a reduction in the company's culpability score under the sentencing guidelines, which is used to determine the company's monetary penalty.[14] The following quotes provide insights into the views of regulators in this area:

> *While the Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees, the critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives.*[15]
>
> *We need to send a message to encourage companies to make the necessary investments in training and controls to prevent this misconduct from happening. The key thing, I think, is tone at the top. Are people at the top sending a message, "Get this business any way you can, I don't care how you get it?" Or are you building a culture in your company that says, "We're going to do it the right way. You're going to get in trouble if you don't follow our rules."*[16]
>
> *The fact is, if you are doing the things you should be doing—whether it is self-policing, self-reporting, conducting proactive risk assessments, improving your controls and procedures, training on the FCPA, or cooperating with an investigation after it starts—you will get a benefit. It may not mean that you or your client will get a complete pass, but you will get a real, tangible benefit.*[17]

Forensic accountants can help companies enhance and execute their compliance remediation programs by considering and assisting in addressing the following areas:

- Broad compliance topics (that is, anti–money laundering, antibribery)
- Limited in-house resources and expertise
- Resistance to change from old-timers and current corporate culture
- Global, decentralized operations
- Identifying high-risk compliance areas and business relationships
- Ongoing monitoring and testing of controls
- Benchmark against other best-in-compliance programs
- Ownership and implementation at local level
- Due diligence on high-risk relationships and activities

---

[14] www.justice.gov/dag/cftf/corporate_guidelines.htm—DOJ.
[15] www.justice.gov/dag/cftf/corporate_guidelines.htm.
[16] Walter Ricciardi, [former] deputy director of the Division of Enforcement of the SEC, *National Law Journal* roundtable, FCPA.
[17] Alice S. Fisher, assistant attorney general, U.S. DOJ, ABA National Institute on the Foreign Corrupt Practices Act, October 16, 2006.

- Formal and regular compliance audit program
- Centralized tracking, monitoring, and reporting

There has been increased pressure on companies to do more with less as a result of declines in sales, budget cuts, and so on. Businesses are also evaluating various economic, legislative, and regulatory programs, their impact on operations and any related compliance and reporting requirements. To navigate this environment, companies need to be creative and proactive in the identification, assessment, and management of risks.

In response to these market dynamics, forensic accountants should continually broaden their approach and service offerings and apply the forensic mindset honed from work on crises and investigations in new and creative ways to help clients address emerging risks and achieve various objectives.

As discussed in this chapter, one of the areas in which the forensic experience can add value is in helping companies develop, test, and monitor key elements of their compliance program. This may include the identification of high-risk areas of operation, the performance of periodic risk assessments, the design, implementation, and possible automation of fraud prevention and detection controls, and assistance with remedial actions, including the development and delivery of training and education programs for board members, management, personnel, and key business partners.

Forensic accountants typically conduct analyses and investigations on behalf of clients responding to a crisis of some sort. A by-product of an investigation is often recommended remedial measures or actions that the company can take to avoid a recurrence. By using the lessons learned from these prior experiences, a forensic accountant can add value to efforts undertaken by companies involved in larger-scale corporate remediation efforts. Such efforts and support can help companies build stronger and more sustainable business practices and provide them with a framework to better evaluate complex relationships and situations and arm them with the information necessary to make better decisions.

A Guide to Forensic Accounting Investigation, Second Edition
By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill

Index